

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

**IN RE NICKELODEON CONSUMER
PRIVACY LITIGATION**

)
) **C.A. 13-MD-2443 (SRC)**
)

) **Judge Stanley R. Chesler**
)

) **FIRST AMENDED**
) **MASTER CONSOLIDATED**
) **CLASS ACTION COMPLAINT**
)

This Document Relates to:

All Actions

I. INTRODUCTION AND OVERVIEW

1. This class action seeks damages and injunctive relief on behalf of all minor children under the age of 13 in the United States who visited Nick.com, owned by Defendant Viacom, Inc., (hereinafter “Viacom”) and which has a target audience of minor children.

2. Specifically, this case is about Defendant Viacom and Defendant Google, Inc.’s (hereinafter “Google”) misuse of Internet technologies (“cookies”) to disclose compile, store and exploit the video viewing histories and Internet communications of minor children throughout the United States in contravention of federal and state law. With neither the knowledge nor the consent of their parents, unique and specific electronic identifying information about each of these children was accessed, stored, and utilized for commercial purposes.

3. This case is brought to enforce the privacy rights of these children, and to enforce the federal and state laws designed to uphold those rights.

II. NATURE OF THE ACTION

4. The named Plaintiffs are minor children under the age of 13 who were registered users of the website Nick.com.

5. The Defendants utilized Internet technologies commonly known as “cookies” to track, record and share the plaintiffs’ and putative class members’ video-viewing histories on Nick.com without plaintiffs’ informed written consent.

6. The Defendants further utilized these technologies to track and record plaintiffs’ and the putative class members’ Internet communications without plaintiffs’ authorization or consent.

7. Plaintiffs are informed and believe the Defendants’ conduct is systematic and class wide.

8. The Defendants’ conduct violated federal and state laws designed to protect the privacy of American citizens, including children. Such conduct gives rise to the following statutory and common law causes-of-action:

- a. Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710, et seq.;
- b. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq.;
- c. Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.;
- d. Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et seq.;
- e. Violation of the California Invasion of Privacy Act, Cal. Penal Code §631(a), et seq.;
- f. Violation of the New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq.;
- g. Intrusion Upon Seclusion; and
- h. Unjust Enrichment.

III. THE PARTIES

A. Plaintiffs

9. Plaintiffs CAF, CTF, MP and TP are minor children under the age of 13 who reside in the State of New Jersey. At all relevant times, they have been registered users of the website Nick.com.

10. Plaintiff T.M. is a minor child under the age of 13 who resides in the State of Illinois. At all relevant times, T.M. has been a registered user of the websites Nick.com.

11. Plaintiff N.J. is a minor child under the age of 13 who resides in the State of Missouri. At all relevant times, N.J. has been a registered user of the website Nick.com

12. Plaintiff AV is a minor child under the age of 13, who resides in the State of New York. At all relevant times, AV has been a registered user of the website Nick.com

13. Plaintiff Johnny Doe is a minor child under the age of 13, who resides in the State of Texas. At all relevant times, he has been a registered user of the website Nick.com,

14. Plaintiff K.T. is a minor child under the age of 13, who resides in the state of Pennsylvania. At all relevant times, K.T. has been a registered user of the website Nick.com

B. Defendant Viacom

15. Defendant Viacom, Inc. is a publicly-traded Delaware corporation with headquarters at 515 Broadway, New York, New York 10036. Defendant Viacom does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

16. Defendant Viacom publicly proclaims its Nickelodeon division to be “the number-one entertainment brand for kids.”¹

¹ Viacom.com, Viacom Company Overview,

C. Defendant Google

17. Defendant Google, Inc. is a publicly traded Delaware corporation with headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Defendant Google does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

18. Google has, by design, become the global epicenter of Internet search and browsing activity. Underscoring its vast Internet reach, Google describes its “mission” as “to organize the world’s information and make it universally accessible and useful.”²

IV. JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendants because all Defendants have sufficient minimum contacts with this District in that they all operate businesses with worldwide reach, including but not limited to the State of New Jersey.

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises in part under federal statutes, namely 18 U.S.C. §2710, et seq. (the Video Privacy Protection Act), 18 U.S.C. §2510, et seq. (the Electronic Communications Privacy Act), 18 U.S.C. § 2701 et seq. (the Stored Communications Act), and 18 U.S.C. § 1030, et seq. (the Computer Fraud and Abuse Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any Defendant.

<http://www.viacom.com/brands/pages/nickelodeon.aspx> (last visited October 7, 2013).

² Google.com, Google Company Overview, <http://www.google.com/about/company> (last visited October 7, 2013).

21. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391 because a substantial amount of the conduct giving rise to this cause of action occurred in this District and because the United States Judicial Panel on Multidistrict Litigation transferred this case to this District for consolidated pretrial proceedings pursuant to Transfer Order in MDL No. 2443, entered on June 11, 2013.

V. FACTS COMMON TO ALL COUNTS

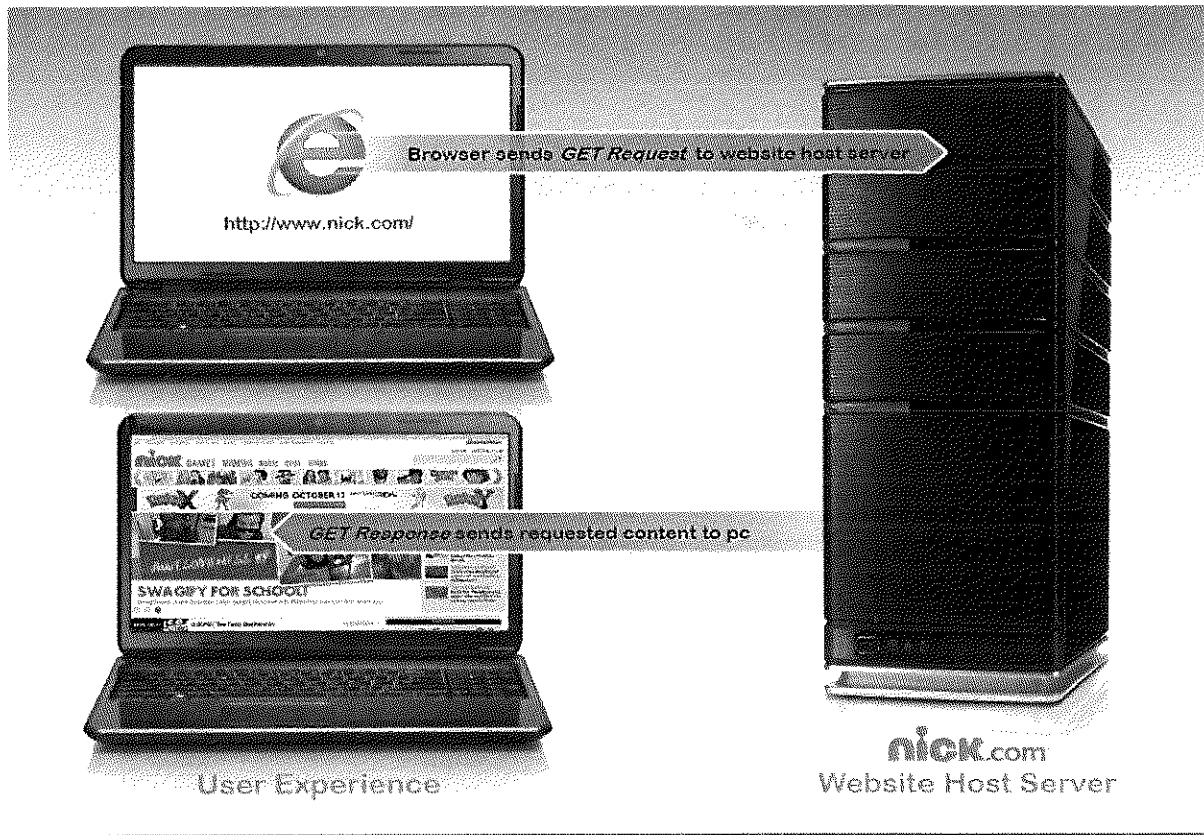
A. How Internet Users Access Websites

23. In order to access and communicate on the Internet, people employ web-browsers such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

24. Every website is hosted by a computer server, which communicates with an individual's web-browser to display the contents of webpages on the monitor or screen of their individual device.

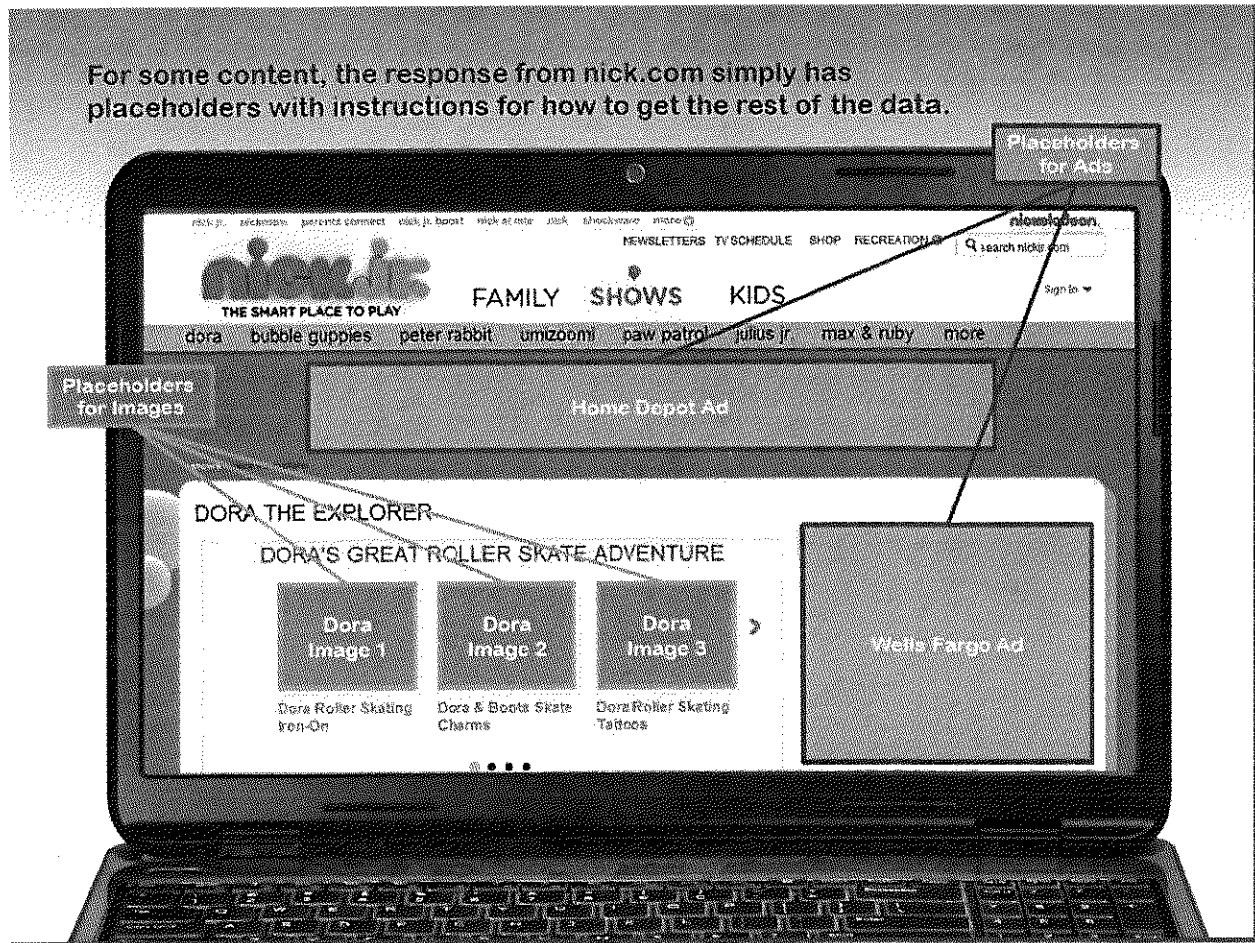
25. The basic command web browsers use to communicate with website servers is called the "GET" command.

26. For instance, when a child types "www.nick.com" into the navigation bar of his or her web-browser and hits "Enter," the child's web browser sends a "GET" command to the Nick.com host server. The "GET" command instructs the Nick.com host server to send the information contained on Nick.com to the child's browser for display. Graphically, the concept is illustrated as follows:



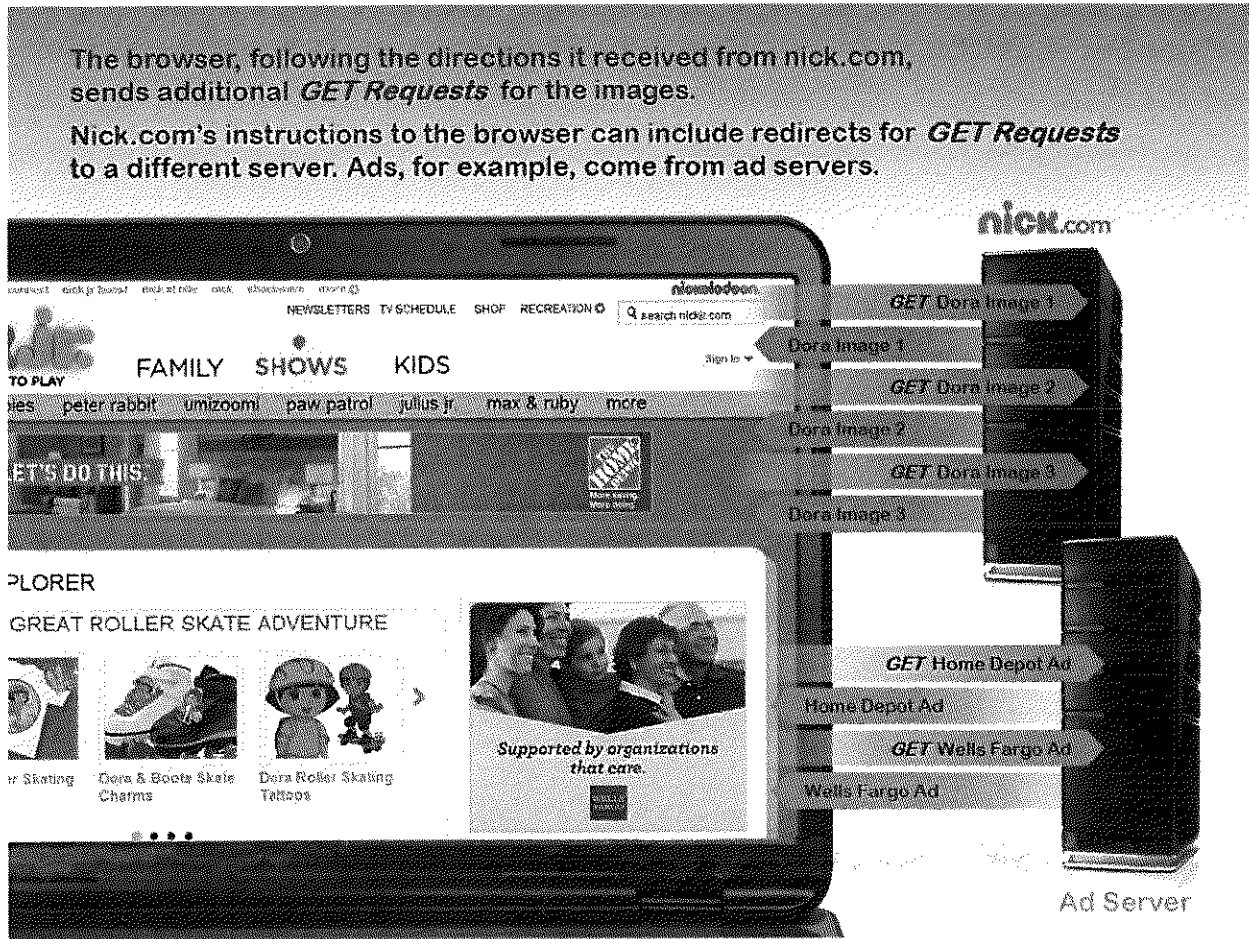
27. Although a single webpage appears on the child's screen as a complete product, a single webpage is in reality an assembled collage of independent parts. Each different element of a webpage – i.e. the text, pictures, advertisements and sign-in box – often exist on distinct servers, which are sometimes operated by separate companies.

28. To display each of these parts of the webpage as one complete product, the host server leaves part of its website blank.



29. Upon receiving a GET command from a child's web browser, the website host server contemporaneously instructs the child's web browser to send other GET commands to other servers responsible for filling in the blank parts of the web page.

30. Those other servers respond by sending information to fill in the blank portions of the webpage.



B. How Targeted Internet Advertising Works

31. In the Internet's formative years, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

32. Computer programmers eventually developed technologies commonly referred to as Internet "cookies," which are small text files that web servers can place on a person's computing device when that person's web browser interacts with the website host server.

33. Cookies can perform different functions; and some cookies were eventually designed to track and record an individual's activity on websites across the Internet.

34. In general, cookies are categorized by: (1) “time” – the length of time they remain on a user’s device; and, (2) “party” – describing the relationship (first or third party) between the Internet user and the party who places the cookie:

a. Cookie Classifications by *Time*

- i. “Session cookies” are placed on a person’s computing device only for the time period during which the person is navigating the website that placed the cookie. The person’s web browser normally deletes session cookies when he or she closes the browser.
- ii. “Persistent cookies” are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a “persistent cookie” can record a person’s Internet browsing history and Internet communications for years. By virtue of their lifespan, persistent cookies can track a person’s communications across the Internet. Persistent cookies are also sometimes called “tracking cookies.”

b. Cookie Classifications by *Party*

- i. “First-party cookies” are set on a person’s device by the website the person intends to visit. For example, Defendant Viacom sets a collection of Nick.com cookies when a child visits Nick.com. First-party cookies can be helpful to the user, server and/or website to assist with security, login and functionality.
- ii. “Third-party cookies” are set by website servers other than the server the person intends to visit. For example, the same child who

visits Nick.com will also have cookies placed on his or her device by third-party web servers, including advertising companies like Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling and targeted advertising.

35. In addition to the information obtained by and stored within third party cookies, third party web servers can be granted access to profile and other data stored within first party cookies.

36. Enterprising online marketers, such as defendants, have developed ways to monetize and profit from these technologies. Specifically, third party persistent “tracking” cookies are used to sell advertising that is customized based upon a particular person’s prior Internet activity.

37. Website owners such as Viacom can now sell advertising space on their web pages to companies who desire to display ads to children that are customized based on the child’s Internet history.

38. Moreover, many commercial websites with extensive advertising allow third-party companies such as Google to serve advertisements directly from third-party servers rather than through the first party website’s server.

39. To accomplish this, the host website leaves part of its webpage blank. Upon receiving a “GET” request from an individual’s web browser, the website server will, unbeknownst to that individual, immediately and contemporaneously re-direct the user’s browser to send a “GET” request to the third-party company charged with serving the advertisements for

that particular webpage.

40. Some websites contract with multiple third-parties to serve ads such that the website will contemporaneously instruct a user's browser to send multiple "GET" requests to multiple third-party websites.

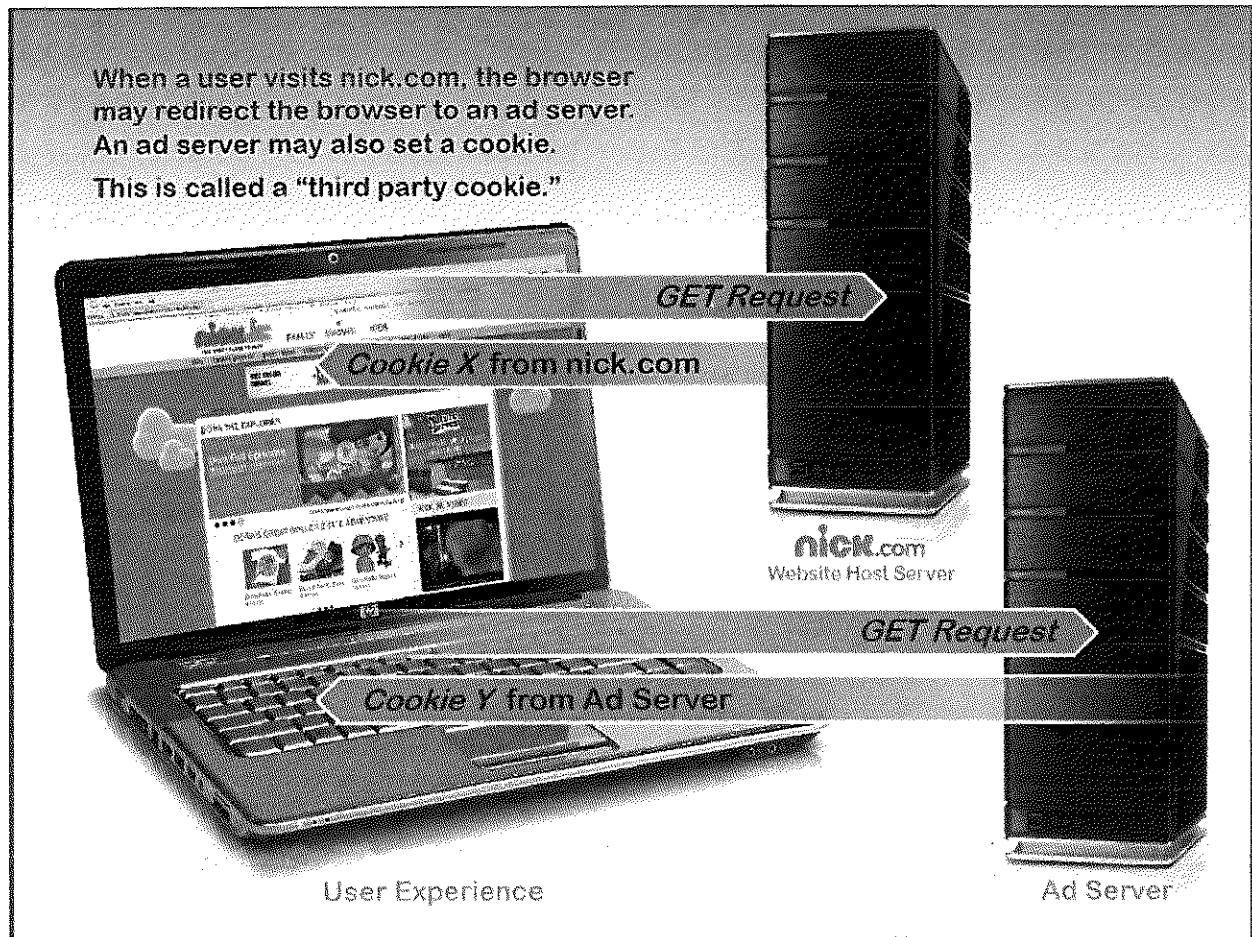
41. In many cases, the third party receives the re-directed "GET" request and a copy of the user's request to the first-party website before the content of the initial request from the first-party webpage appears on the user's screen.

42. The transmission of such information is contemporaneous to the user's communication with the first-party website.

43. The third-party server then responds by sending the ad to the user's browser – which then displays it on the user's device.

44. In the process of placing advertisements, third-party advertising companies also implant third-party cookies on individuals' computers. They further assign each specific user a unique numeric or alphanumeric identifier that is associated with that specific cookie.

45. The entire process occurs within milliseconds and the web page appears on the individual's web browser as one complete product, without the person ever knowing that multiple GET requests were executed by the browser at the direction of the web site server, and that first party and third party cookies were placed. Indeed, all the person has done is type the name of a single web page into his or her browser. Graphically, the concept is illustrated as follows:



46. Because advertising companies serve advertisements on multiple sites, their cookies also allow them to monitor an individual's communications over every website and webpage on which the advertising company serves ads. And because that cookie is associated with a unique numeric or alphanumeric identifier, the data collected can be utilized to create detailed profiles on specific individuals.

47. By observing the web activities and communications of tens of millions of Internet users, advertising companies, including Defendant Google, build digital dossiers of each individual user and tag each individual user with a unique identification number used to aggregate their web activity. This allows for the placement of "targeted" ads.

C. The Value of the Personal Information Defendants Collect

48. To the advertiser, targeted ads provided an unprecedented opportunity to reach potential consumers. The value of the information that Defendants take from people who use the Internet is well understood in the e-commerce industry. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.³

49. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute, Christopher Soghoian, noted:

The dirty secret of the Web is that the “free” content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.

Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.⁴

50. In the behavioral advertising market, “the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him.”⁵

51. In general, behaviorally targeted advertisements based on a user’s tracked internet

³ Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

⁴ Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

⁵ <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> at 37 (last visited Aug. 12, 2014).

activity sell for at least *twice* as much as non-targeted, run-of-network ads.⁶

52. Upon information and belief, most of the Defendants' advertising clients pay on a cost-per-click basis.

53. The Defendants also offer cost-for-impression ads, which charge an advertising client each time the client's ad displays to a user.

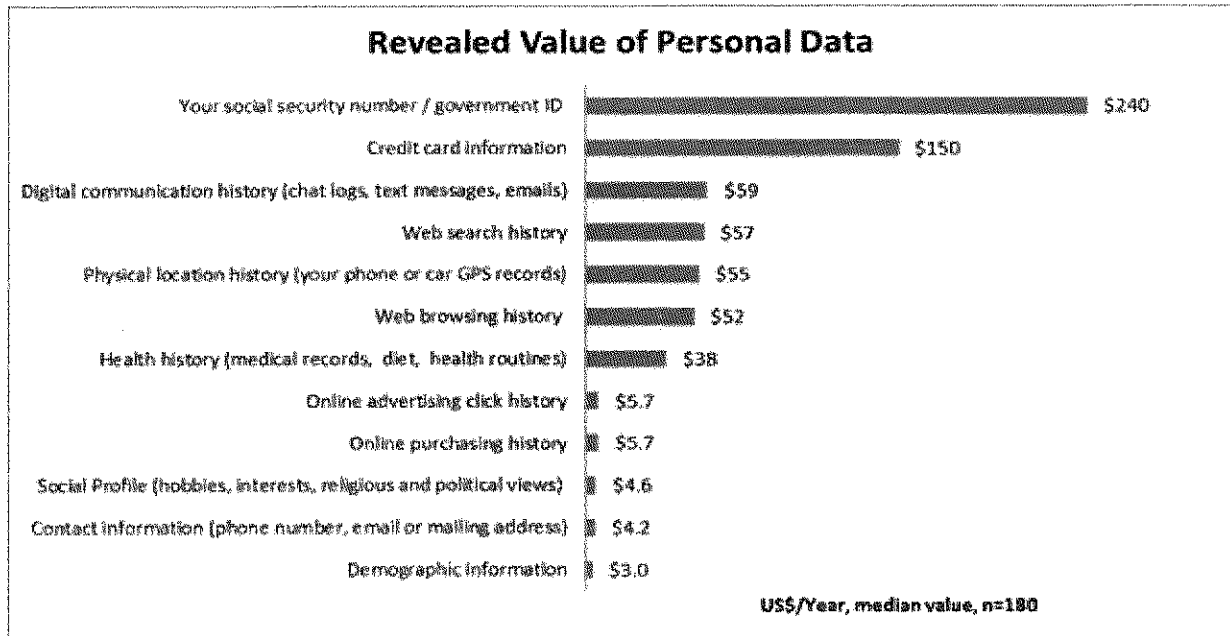
54. In general, behaviorally-targeted advertisements produce 670 percent more clicks on ads per impression than run-of-network ads. Behaviorally-targeted ads are also more than twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.⁷

55. The cash value of users' personal information can be quantified. For example, in a recent study authored by Tim Morey, researchers studied the value that 180 Internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately \$4.20 per year. Demographic information was valued at approximately \$3.00 per year. Web browsing histories were valued at a much higher rate: \$52.00 per year. The chart below summarizes the findings⁸:

⁶ NetworkAdvertising.org, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (last visited September 16, 2013).

⁷ Howard Beales, *The Value of Behavioral Advertising*, 2010 http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited September 16, 2013).

⁸ Tim Morey, *What's Your Personal Data Worth?*, January 18, 2011, <http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html> (last visited September 16, 2013).



56. In 2012, Defendant Google convened a panel called “Google Screenwise Trends” through which Google paid Internet users to track their online communications through gift cards, with most valued at \$5. Though it is unclear whether Google continues to operate Screenwise Trends in the United States,⁹ the project remains active in the U.K., where users are paid £15 for staying with Screenwise Trends for 30 days after sign-up and an additional £5 for every 90 days users remain with the panel.¹⁰ Google’s Screenwise Trends program demonstrates conclusively that Internet industry participants, including the Defendants, recognize the enormous value in tracking user’s Internet communications.

57. Targeting advertisements to children adds *more* value than targeting to adults because children are generally unable to distinguish between content and advertisements. This is especially true in the digital realm where children are less likely to identify and counteract the

⁹ See <https://www.screenwisepanel.com/member/Index.aspx?ReturnUrl=%2fmember>, (last visited Sept. 25, 2013), which plaintiffs believe is the sign-in page for Screenwise Trend users in the United States, indicating the program is still in existence.

¹⁰ See <https://www.screenwisetrendspanel.co.uk/nrg/rewards.php> (last visited Sept. 25, 2013).

persuasive intent of advertising. This results in children, especially those below the age of 8, accepting advertising information contained in commercials “uncritically . . . [and as] truthful, accurate, and unbiased.”¹¹

58. An investigation by the Wall Street Journal revealed that “popular children’s websites install more tracking technologies on personal computers than do the top websites aimed at adults.”¹² In particular, Viacom disclosed substantially more information to third-party tracking companies than typical adult websites. According to the investigation in September 2010, Viacom placed 92 tracking cookies on the Nick.com website, a total which is 144 percent more than the average tracking cookies placed on the 50 most popular adult websites in the United States.¹³

D. Internet Tracking is Not Anonymous

59. Though industry insiders claim publicly that tracking is anonymous, experts in the field disagree. For instance, in a widely cited blog post for The Center for Internet and Society at Stanford Law School titled “There is No Such Thing as Anonymous Online Tracking,” Professor Arvind Narayanan explained:

¹¹ Report of the APA Task Force on Advertising and Children at 8 available at <http://www.apa.org/pi/families/resources/advertising-children.pdf> (last visited August 12, 2014). See also *Research on Child Development: Implications of How Children Understand and Cope with Digital Marketing*, Louis J. Moses. Available at: http://digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (last visited August 12, 2014).

¹² Steve Stecklow, *On the Web, Children Face Intensive Tracking*, THE WALL STREET JOURNAL, September 17, 2010, <http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html> (last visited September 16, 2013).

¹³ See <http://blogs.wsj.com/wtk-kids/> for statistics on Nick.com and other children’s sites (last visited July 30, 2014); see <http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404> for tracking statistics on the most popular adult websites (last visited July 30, 2014).

In the language of computer science, clickstreams – browsing histories that companies collect – are not anonymous at all; rather, they are pseudonymous. The latter term is not only more technically appropriate, it is much more reflective of the fact that at any point after the data has been collected, the tracking company might try to attach an identity to the pseudonym (unique ID) that your data is labeled with. Thus, identification of a user affects not only future tracking, but also retroactively affects the data that's already been collected. Identification needs to happen only once, ever, per user.

Will tracking companies actually take steps to identify or deanonymize users? It's hard to tell, but there are hints that this is already happening: for example, many companies claim to be able to link online and offline activity, which is impossible without identity.¹⁴

60. Moreover, any company employing re-identification algorithms can precisely identify a particular consumer:

It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.

The versatility and power of re-identification algorithms imply that terms such as “personally identifiable” and “quasi-identifier” simply have no technical meaning. While some attributes may be uniquely identifying on their own, any attribute can be identifying in combination with others.¹⁵

61. The Federal Trade Commission has recognized the impossibility of keeping data derived from cookies and other tracking technologies anonymous, stating that industry, scholars, and privacy advocates have acknowledged that the traditional distinction between the two

¹⁴ Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, The Center for Internet and Society Blog, July 28, 2011, <http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking> (last visited September 16, 2013).

¹⁵ Arvind Narayanan, “*Privacy and Security Myths of Fallacies of ‘Personally Identifiable Information,’*” Communications of the ACM, June 2010, http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf (last visited September 16, 2013).

categories of data [personally identifiable information and anonymous information] has eroded and is losing its relevance.¹⁶

62. For example, in 2006, AOL released a list of 20 million web search queries connected to “anonymous” ID numbers, including one for user No. 4417749. Researchers were quickly able to identify specific persons with the so-called anonymous ID numbers. As explained by the New York Times:

The number was assigned by the company to protect the searcher’s anonymity, but it was not much of a shield.

. . . .
[T]he detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines – and how risky it can be for companies like AOL, Google, and Yahoo to compile such data.”¹⁷

63. Another technological innovation is the use of “browser fingerprinting,” which allows websites to “gather and combine information about a consumer’s web browser configuration – including the type of operating system used and installed browser plug-ins and fonts – to uniquely identify and track the consumer.”¹⁸

64. By using browser-fingerprinting alone, the likelihood that two separate users have the same browser-fingerprint is one in 286,777, or 0.000003487 percent.¹⁹ This accuracy is increased substantially where the tracking company also records a user’s IP address and unique

¹⁶ FTC.gov, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, December 2010, <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> (last visited September 16, 2013).

¹⁷ Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times., Aug. 9, 2006, <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=print> (last visited September 16, 2013).

¹⁸ *Protecting Consumer Privacy in an Era of Rapid Change* at 36.

¹⁹ *How Unique Is Your Web Browser?* by Peter Eckersley, available at <https://panopticklick.eff.org/browser-uniqueness.pdf> (last visited July 28, 2014).

device identifier.

65. Another recent innovation, as Prof. Narayanan predicted, is for companies to connect online dossiers with offline activity. As described by one industry insider:

With every click of the mouse, every touch of the screen, and every add-to-cart, we are like Hansel and Gretel, leaving crumbs of information everywhere. With or without willingly knowing, we drop our places of residence, our relationship status, our circle of friends and even financial information. Ever wonder how sites like Amazon can suggest a new book you might like, or iTunes can match you up with an artist and even how Facebook can suggest a friend?

Most tools use first-party cookies to identify users to the site on their initial and future visits based upon the settings for that particular solution. The information generated by the cookie is transmitted across the web and used to segment visitors' use of the website and to compile statistical reports on website activity. This leaves analytic vendors – companies like Adobe, Google, and IBM – *the ability to combine online with offline data*, creating detailed profiles and serving targeted ads based on users' behavior.²⁰

66. On information and belief, the Defendants in this case are able to link online and offline activity to identify specific users, including the plaintiffs and children that form the putative class. The Defendants, in fact, have marketed their ability to target individual users by connecting data obtained from first-party and third-party cookies.

- a. Specifically, Defendant Viacom holds itself out to advertisers as being able to target users with “pinpoint accuracy” to reach “specific audiences on every digital platform” by “connecting the dots between first and third-party data to get at user attributes including interests, behaviors, demo,

²⁰ Tiffany Zimmerman, *Data Crumbs*, June 19, 2012, <http://www.stratigent.com/community/analytics-insights-blog/data-crumbs> (last visited September 16, 2013) (emphasis added).

geolocation, and more.”²¹ Viacom does this through its “Surround Sound” service powered through Adobe’s Audience Manager product. Viacom Vice President for Digital Products, Josh Cogswell, has said publicly the product can be used to target “kids” and, regarding Viacom’s audience, “We know who you are across our sites.”

- b. Defendant Google announced a new service in December 2012 called the DoubleClick Search API Conversion Service that will allow advertisers to integrate offline activity with online tracking.²²

67. Viacom and Google use the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage and the content of the their web communications, including, but not limited to, videos requested and obtained.

E. Web-Browsers and Internet Service Provider Privacy Policies Prohibit Unlawful and Non-Consensual Tracking of User Communications

68. Internet Service Providers (ISPs) provide connection services which allow consumers to send, and receive electronic communications on the Internet.

69. ISPs operate under Privacy Policies which prohibit users from engaging in unlawful or non-consensual tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts.. For example:

- a. AT&T’s “Acceptable Use Policy” includes a general prohibition against using the services “in any way that is unlawful ... or a violation of

²¹ Viacom.com Viacom Blog, “Serving Advertisers in Surround Sound,” March 26, 2012 <http://blog.viacom.com/2012/03/serving-advertisers-in-surround-sound-2/> (last visited September 16, 2013), “Kids” admission at 5:17 of video. “We know who you are across our sites,” at 6:25 of video.

²² Google.com, DS API Interface – Conversion Service Overview, <https://support.google.com/ds/answer/2604604?hl=en> (last visited September 16, 2013).

privacy.” In addition, it specifically prohibits any use which would violate any applicable criminal, civil, or administrative law and provides that users “may not (use AT&T IP services to) ... gain unauthorized access to ... another party’s server, network, network access, personal computer, or control devices, software or data.” This prohibition includes, but is not limited to any “unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of email addresses” or “gaining access to ... any host, network, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network.”²³

- b. Time’s Warner’s “Acceptable Use Policy” provides that subscribers “agree to use the ISP service only for lawful purposes” and that its “ISP service may not be used to breach the security, the computer, the software, or the data of any person or entity.”²⁴
- c. CenturyLink’s “Acceptable Use Policy” provides that users “may access and use the Network only for lawful purposes.” In addition, it prohibits “unauthorized monitoring of data or traffic on any network or system without the express prior authorization of the owner of the system or network” and “disseminating ... harmful content, including, without

²³ See <http://www.corp.att.com/aup/> (last visited July 28, 2014).

²⁴ See http://help.twcable.com/twc_misp_aup.html (last visited July 28, 2014).

limitation ... computer or other programming routines that may ... secretly intercept ... any ... data or personal information.”²⁵

- d. Verizon’s “Acceptable Use Policy” provides that users may not “access without permission or right the accounts or computer systems of others.”²⁶
- e. Charter’s “Acceptable Use Policy” provides that users may not use the service to “violate any applicable federal, state, local, or international laws (including, but not limited to, the Children’s Online Privacy Protection Act.)” It further prohibits use of the Service “to commit a crime” or to gain “unauthorized access to any computer, ... data, information, or any other proprietary material.”²⁷
- f. Comcast’s “Acceptable Use Policy” for business users provides that such users shall not use the service to “undertake or accomplish any unlawful purpose” which includes conduct which “in any way constitutes or encourages” commission of a “criminal offense” or which “otherwise violate[s] any local, state, federal, or non-U.S. law, order, or regulation.” In addition, users may not “access any other person’s computer or computer system, network, software, or data without his or her knowledge and consent” or participate “in the collection of very large numbers of

²⁵ See

<http://www.centurylink.com/Pages/AboutUs/Legal/AcceptableUse/acceptableUsePolicy.jsp> (last visited July 28, 2014).

²⁶ See

https://my.verizon.com/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=AcceptableUse (last visited July 28, 2014).

²⁷ See <https://www.charter.com/browse/content/policies-comm-acceptable-use> (last visited July 28, 2014).

email addresses, screen names, or other identifiers of others” without their prior consent.²⁸

- g. Plaintiffs are not aware of any ISP in the United States which consents to use of its service to engage in criminal or otherwise unlawful acts.

70. Web-browsers are software services which allow consumers to send and receive electronic communications on the Internet. As described by Defendant Google, the web-browser is a service where users “spend much of their time working[.] ... We search, chat, email and collaborate in a browser. And in our spare time, we shop, bank, read news and keep in touch with friends – all using a browser.”²⁹

71. Web-browsing services include Terms of Use which prohibit users from engaging in unlawful or unauthorized tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts. For example:

- a. Defendant Google’s Chrome browser Terms of Service provides that users “agree to use the services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation, or generally accepted practices or guidelines in the relevant jurisdictions.”³⁰

²⁸ See <http://business.comcast.com/customer-notifications/acceptable-use-policy> (last visited July 28, 2014).

²⁹ See <http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html> (last visited July 28, 2014).

³⁰ See https://www.google.com/intl/en_US/chrome/browser/privacy/eula_text.html (last visited July 28, 2014).

- b. Microsoft Internet Explorer's Terms of Service provides that users "may not use the service to try to gain unauthorized access to any service, data, account, or network by any means."³¹
- c. Apple Safari's Terms of Use agreement provides that users may not "exploit the Services in any unauthorized way, including but not limited to, ... trespass." Users "further agree not to use the Services in any manner to harass, abuse, stalk, threaten, defame, or otherwise infringe or violate the rights of another party."

72. Web-browser Terms of Use also typically permit the web-browser provider to access a user's computer for purposes of providing better browser services:

- a. Google Chrome informs users that, "From time to time, Google Chrome may check with remote servers (hosted by Google or by third parties) for available updates to extensions, including but not limited to bug fixes or enhanced functionality. You agree that such updates will be automatically requested, downloaded, and installed without further notice to you."³²
- b. Microsoft Internet Explorer informs users that its browser "connect[s] to Microsoft and service provider computer systems over the Internet." These connections include utilization of Microsoft's "Customer Experience Improvement Program" which "collects basic information about your computer and how you use Internet Explorer to help us improve the quality, reliability, and performance of our software and services. CEIP

³¹ See <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/end-user-license-agreement> (last visited July 28, 2014).

³²

reports generally include information about your hardware configuration, a unique identifier generated by CEIP, performance and reliability data (such as how quickly the software responds when you click a button), and program use (such as which features you use most often).”

- c. Apple Safari requires users to “agree that Apple and its subsidiaries and agents may collect, maintain, process and use diagnostic, usage and related information, including but not limited to information about your computer, system, and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any) related to the Apple Software.”

F. How Viacom and Google Track Children’s Internet Use

73. Immediately upon the Plaintiffs’ first communication with the Viacom children’s websites, Defendant Viacom automatically placed its own first party cookies on the computing devices of the Plaintiffs.

74. Additionally, immediately upon the Plaintiffs’ first communication with the Viacom children’s websites, Viacom knowingly permitted Defendant Google to place its own persistent third-party tracking cookies on the computing devices of the Plaintiffs and then transmitted the Plaintiffs’ subsequent communications to Google through those persistent tracking cookies and other information, or, in cases where Google’s third-party cookies were already present on the Plaintiffs’ computing devices, Viacom transmitted to Google the Plaintiffs’ communications through the persistent tracking cookies which already existed on the user’s device by virtue of Plaintiffs having visited another website affiliated with Google.

75. Viacom allowed Google to place and/or access cookies from its doubleclick.net

domain.

76. Upon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first party cookies.

77. The placement and disclosure of information in or associated with these cookies occurred before either the Plaintiffs or their legal guardians had the opportunity to consent to their placement and/or access to the Plaintiffs' Internet communications.

78. Google's third-party cookies tracked, among other things, the URLs (Uniform Resource Locators—also known as a web address) visited by the Plaintiffs, the Plaintiffs' respective IP addresses and each Plaintiff's browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with Viacom's children's websites.

79. The URLs visited by plaintiffs and putative class members contain substantive and often sensitive content. For example:

- a. A Plaintiff minor child seeking information about "what to do if my parents are getting divorced" may enter that search term in the Google search engine.
- b. The second result in Google's search engine is a hyperlink with the Subject Line: "How to Deal With Your Parents' Divorce: 12 Steps."
- c. By clicking on the link and affirmatively indicating through the web-browser that they seek information on their parents' divorce, the browser would send a communication on the Plaintiffs' behalf to a webpage with the URL, <http://www.wikihow.com/Deal-With-Your-Parents'-Divorce>.

- d. In response to the Plaintiffs' "GET" request communication seeking information on what to do if their parents get divorced, the website WikiHow.com returns a communication which includes an essay with 12 detailed steps a child could take if their parents were getting a divorce.
- e. Google places cookies on WikiHow.com with the same unique identifiers as the cookies placed on the Viacom children's websites.
- f. The following picture illustrates WikiHow's communication regarding "what to do if my parents are getting divorced."



80. Viacom further disclosed to Google at least the following about each Plaintiff who was a registered user of Viacom's children's websites: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites, and (11) the DoubleClick persistent cookie identifier.

81. By disclosing the above information to Google, Viacom has knowingly disclosed information which, without more, when disclosed to Google, links specific persons with their

online communications and data, based on information that Google already has in its possession.

82. Viacom and Google used the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage, including videos requested and obtained.

G. How Google Identifies Specific Individuals and Their Families

83. Defendant Google publicly admits that it can identify web users with Google's DoubleClick.net cookies:

For itself, Google identifies users with cookies that belong to the doubleclick.net domain under which Google serves ads. For buyers, Google identifies users using a buyer-specific Google User ID which is an encrypted version of the doubleclick.net cookie, derived from but not equal to that cookie.³³

84. Google has a ubiquitous presence on the Internet. In October 2012, DoubleClick cookies were present on 69 of the 100 most popular websites.³⁴ In July 2013, experts estimated Google accounted for 25 percent of all Internet traffic running through North American ISPs, an amount larger than the combined traffic of Facebook, Netflix, and Instagram.³⁵ In addition to DoubleClick, Google owns and operates:

- a. The world's third most popular social network at plus.google.com,³⁶ for which Google claims to have over 300 million users;
- b. The world's most popular search engine at Google.com, which, according to comScore, processed 12.1 billion searches in the United States in June 2014, or 68 percent of all U.S. Internet searches.³⁷

³³ Google.com Google Developer Cookie Guide, <https://developers.google.com/adexchange/rtb/cookie-guide> (last visited September 16, 2013).

³⁴ See <http://www.law.berkeley.edu/privacycensus.htm> (last visited July 24, 2014).

³⁵ See <http://www.wired.com/2013/07/google-internet-traffic/> (last visited July 29, 2014).

³⁶ According to Alexa, Facebook and LinkedIn have more users than Google Plus.

- c. The world's most popular email service at Gmail.com, which, as of June 2012, had more than 250 million users worldwide;³⁸
- d. The world's most popular video service at YouTube.com, which, according to comScore, had 153 million unique video viewers in June 2014;³⁹
- e. A mapping service called Google Maps at www.google.com/maps that includes applications which track the precise geo-locations of users, and which is according to some estimates, the most popular smartphone app in the world;
- f. An online personal photography website called Picasa at picasa.google.com;
- g. Its own electronic store called Play at play.google.com;
- h. Its own web-browser called Google Chrome;
- i. an online software suite called Google Apps that, as of June 2012, was used by 66 of the top 100 universities in the United States, government institutions in 45 states, and a total of 5 million businesses,⁴⁰ and
- j. Its own mobile phone platform called Android which is the most highly used platform in the United States and allows Google to track user movements, app usage, and phone calls.

85. Google collects users' IP addresses, unique device identifiers, and user account

³⁷ See <https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-June-2014-US-Search-Engine-Rankings> (last visited July 29, 2014).

³⁸ See <http://googleblog.blogspot.com/2012/06/chrome-apps-google-io-your-web.html> (last visited July 24, 2014).

³⁹ See <http://ir.comscore.com/releasedetail.cfm?ReleaseID=860971> (last visited July 29, 2014).

⁴⁰ *Id.*

Information through all of the services listed above. In addition, it tracks use of these services with persistent cookie identifiers. For example:

- a. Google's social-network at Google Plus tracks users with cookies from DoubleClick with the same persistent identifier it uses to track at Nick.com. In addition to DoubleClick cookies, Google tracks its social network users with cookies from plus.google.com, clients6.google.com, and talkgadget.google.com.
- b. Google's search engine tracks users with cookies from the main Google.com domain and from Google's social network at plus.google.com.
- c. Google's email service at Gmail tracks users with cookies from mail.google.com and from Google's social network at plus.google.com.
- d. Google's video service at YouTube.com tracks users with cookies from DoubleClick with the same persistent identifier that it uses to track user at Nick.com. In addition to DoubleClick cookies, Google tracks YouTube users with cookies from its social network at plus.google.com, apis.google.com, gg.google.com, and clients6.google.com.
- e. Google's map service tracks users with cookies from google.com and receives precise geo-location data from users utilizing its mapping services.
- f. Google's electronic storage service called Drive tracks users with cookies from its social network at plus.google.com, and the subdomains drive.google.com and docs.google.com.

- g. Google's electronic store Play tracks users with cookies from its social networking site at plus.google.com.

86. Use of Gmail and the social network Google Plus requires registration, a process through which Google obtains a user's first and last name, hometown, email address, and other personal information about each user.

87. Other Google services collect users' first and last names, hometowns, email addresses, and other personal information when the user signs up as a member for those services.

88. Google admits that it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user account information. Its current privacy policy states that:

- a. It "may collect device-specific information (such as [a user's] hardware model, operating system version, unique device identifiers, and mobile network information including phone number)" and "may associate ... device identifiers or phone number[s] with [a user's] Google Account."⁴¹
- b. It may "automatically collect and store certain information in server logs. This may include: ... search queries, ... Internet protocol address, ... device event information such as ... hardware settings, browser type, browser language, the data and time of your request and referral URL," and "cookies that may uniquely identify your browser or your Google Account."⁴²

89. Google's current Privacy Policy is substantially similar to the one in effect at the time the Plaintiffs' initially filed suit in this case regarding its collection of information. The policy in effect at the time Plaintiffs' filed suit provided as follows:

⁴¹ See <http://www.google.com/policies/privacy/> (last visited July 24, 2014).

⁴² Id.

Device information

We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

Log information

When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

- details of how you used our service, such as your search queries.
- telephone log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account.

Location information

When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

Unique application numbers

Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

Local storage

We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

Cookies and anonymous identifiers

We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

90. Google's Privacy Policy in effect today differs in one key respect from the Policy in effect at the time Plaintiff's filed suit in this case. Google's current Privacy Policy acknowledges that it has the information to connect DoubleClick cookie information with personal information collected from its other services, but promises not to. Google informs users:

We may combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

91. Google's Privacy Policy promise not to combine DoubleClick cookie information with personally identifiable information was not in place until March 1, 2012.⁴³ Because Plaintiff's filed suit in December 2012, Viacom's disclosures to Google were made for a significant period of time without any public commitment by Google that it would not use the information disclosed by Viacom.

92. On March 1, 2012, Google publicly announced that it would be commingling information obtained from Google users across Google accounts. In a company blog post by Alma Whitten, Google's Direct of Privacy, Product, and Engineering, the company announced:

Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products[.]⁴⁴

93. In addition to these websites and services listed above, Google advertises a "cookie matching" service for ad-buyers that permits buyers to match their own cookie with a DoubleClick persistent cookie identifier assigned to a user by Google. Google explains the

⁴³ The changes to Google's Privacy Policy as of March 1, 2012 are highlighted here: <http://www.google.com/policies/privacy/archive/20111020-20120301/> (last visited July 24, 2014).

⁴⁴ See <http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html>. (last visited July 25, 2014).

process as follows:

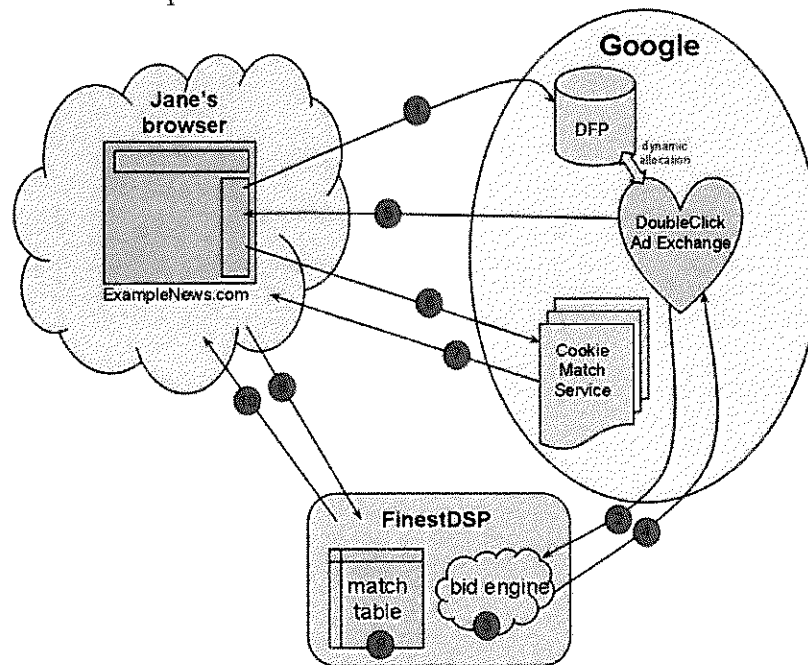
How would cookie matching look to a typical web user, and what's happening behind the scenes? Let's take a look at two scenarios.

Scenario 1: Cleared cookies

Jane clears her cache of all cookies. She then visits the homepage of ExampleNews.com.

Here's what happens:

1. ExampleNews.com renders, and calls ads from Google (DoubleClick for Publishers).
2. Because the ad unit is eligible for dynamic allocation, Ad Exchange sends bid request to FinestDSP (among other DSPs).
3. FinestDSP process the bid request in its bid engine, and sends its bid response to Ad Exchange.
4. FinestDSP wins the auction, and sends an ad and a match tag (pixel) to Ad Exchange.
5. Ad Exchange serves FinestDSP's ad and match tag to Jane, and also sets Jane's DoubleClick cookie.
6. The match tag calls Google's Cookie Match Service.
7. The Cookie Match Service reads Jane's DoubleClick cookie, and sends a redirect to FinestDSP with google_user_id set.
8. The browser loads FinestDSP's URL.
9. FinestDSP generates a cookie, which it stores against Jane's google_user_id in its match table.
10. FinestDSP drops its cookie in Jane's browser and responds to the redirect with an invisible 1x1 pixel.



Scenario 2: Buyer and DoubleClick cookies

A week after Scenario I, Jane visits ExampleNews.com again. Now that Jane has both buyer and DoubleClick cookies on her machine, let's see how matching works.

1. The web page renders, executing the HTML code's call to Google for ads.
2. During the ad auction, DoubleClick Ad Exchange sends a bid request to an RTB buyer, FinestDSP, giving that buyer the option of bidding on the impression.
3. The buyer receives the bid request with impression information and the google_user_id.
4. FinestDSP looks up the google_user_id in its match table to find the cookie created a week earlier (in Scenario I).
5. Based on the information associated with its cookie, FinestDSP decides to bid on the impression, and wins the auction.
6. Jane might see an ad tailored to her interests, again based on information that FinestDSP possesses.

94. Defendant Google admits that IP addresses and cookie information are not anonymous to Google. In fact, Google promises users it will scrub full IP addresses and cookie information from its records after 9 or 18 months in order to “anonymize” user data:

Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. *We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).* If you have Search History enabled, this data may also be stored in your Google Account until you delete the record of your search. *Emphasis added.*

95. Google has further admitted that IP addresses are personal information where the IP address is capable of being tied to an individual by a company. On Google’s Public Policy blog in 2008, then Google software engineer Alma Whitten explained:

[I]s an IP address personal data, or, in other words, can you figure out who someone is from an IP address? A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you’re an ISP and you assign an IP address to a computer that connects under a particular subscriber’s account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the

human beings behind these number strings.⁴⁵

96. Google has more information about Internet users than the ISPs identified by Whitten. Each separate Google product logs and keeps track of different categories of information about Internet users, including, but not limited to the following list:

- a. first and last names,
- b. home or other physical address,
- c. precise current locations of users through GPS,
- d. IP addresses,
- e. telephone numbers,
- f. lists of contacts,
- g. the content of Gmail users' Gmail messages,
- h. search history at Google.com and YouTube,
- i. web-surfing history,
- j. Android device activity, and
- k. all activity on Google's social network called Google Plus.

97. In the case of Nick.com, Google occupies the role of the ISP because it knows user's full names, hometowns, specific geographic locations, email addresses, and more.

98. Viacom is aware of Google's ubiquitous presence on the Internet and its tracking of users across DoubleClick partner websites like Nick.com and Google's own websites at Google.com, Google Plus, YouTube.com, Gmail.com, and Play.Google.com, among others, where Google connects user IP addresses, unique device identifiers, and persistent cookie identifiers to Google account information.

⁴⁵ See <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html> (last visited July 24, 2014).

99. As a result of Google's ubiquitous presence on the Internet, the information Viacom discloses to Google personally identifies the plaintiffs.

H. Google's Internal Position on Privacy.

100. Former Google CEO and current company Executive Chairman Eric Schmidt described Google's privacy plan policy aptly in 2010. "Google's policy," Schmidt said, "is to get right up to the creepy line and not cross it." As detailed below, Google has a history of drawing a line on privacy – and then later crossing right over it.

101. Despite Google's promise not to connect DoubleClick information with Google Account information, Google reserves the right to change its Privacy Policy "from time to time" and has a history of exercising this provision.

102. Android Privacy Reversal – Prior to Google's March 2012 announcement that it would commingle user information across Google accounts, it had promised purchasers of mobile phones with Android that, while "[c]ertain applications or features of your Android-powered phone may cause other information to be sent to Google but in a fashion that cannot be identified with you personally" and that "[y]our device may send us location information (for example, Cell ID or GPS information) that is not associated with your [Google] Account."

103. Search Privacy Reversal – Google's March 2012 announcement resulted in a similar shift for search results. In 2009, Google had promised:

Previously, we only offered Personalized Search for signed-in users, and only when they had Web History enabled on their Google Accounts. What we're doing today is expanding Personalized Search so that we can provide it to signed-out users as well. This addition enables us to customize search results for you based upon 180 days of search activity linked to an anonymous cookie in your browser. It's completely separate from your Google Account and Web History (which are only available to signed-in users).

104. Gmail Privacy Reversal – Google's March 2012 announcement also required a

shift in Gmail policy. Prior to March 2012, Google's Gmail Legal Notice provided that it would "not use any of your content [defined to include "any text, data, information, images, photographs, music, sound, video, or other material, that you upload, transmit, or store in your Gmail account"] for any purpose except to provide you with the Service." With the introduction of the new policy, Google eliminated this provision of its Gmail Legal Notice.

105. Google Hid Plans for Privacy Reversals for Two Years – Prior to March 2012, Google did not give any public indications that it was in the process of changing company policy to commingle all user data across its Search, Gmail, YouTube, Maps, Docs, Picasa, Play, Android, and other services. But this shift to share information across all Google platforms actually began at least as early as May 2010, when Google executives decided to engage in a plan it called "Emerald Sea" which involved eliminating then existing barriers between Google properties.

106. Catching Up to Facebook – "Emerald Sea" was driven in large part by the Google's desire to better compete with Facebook to create detailed digital dossiers of its users.

107. James Whittaker, a former Google Engineering Director, described Google's motivation in a public explanation of his resignation from the company:

It turns out that there was one place where the Google innovation machine faltered and that one place mattered a lot: competing with Facebook. ... Like the proverbial hare confident enough in its lead to risk a brief nap, Google awoke from its social dreaming to find its front runner status in ads threatened. ... Google could still put ads in front of more people than Facebook, but Facebook knows so much more about those people.

Advertisers and publishers cherish this kind of personal information, so much so that they are willing to put the Facebook brand before their own. Exhibit A: www.facebook.com/nike, a company with the power and clout of Nike putting their own brand after Facebook's? No company has ever done that for Google and

Google took it personally.⁴⁶

108. Unlike Facebook, prior to the commingling of information and creation of Google Plus, Google could not create nearly as total a picture of its users for advertisers.

I. Viacom Disclaims Any Control Over Use of Information It Discloses to Google

109. In its own Privacy Policy for Nickelodeon websites that Viacom filed as Exhibit D in response to Plaintiff's First Consolidated Complaint (and which is not valid for the minor children plaintiffs in this case or for purposes of the VPPA), Viacom disavows any control over Google's practices, stating that "the use of [tracking] technology by these third parties is within their control and not the Nickelodeon sites. Even if we have a relationship with a third party, we do not control those sites or their policies and practices regarding your information[.]"⁴⁷

J. Viacom's Disclosures to Google are Not Necessary for Nick.com

110. Defendant Google's DoubleClick cookies are not necessary for Defendant Viacom to render any services on Nick.com.

111. On or about August 1, 2014, Defendant Viacom revamped its Nick.com website. As of August 7, 2014, based on plaintiffs' investigation, Defendant Viacom no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google.⁴⁸

K. What Viacom and the Third Party Tracking Defendants Knew About the Gender and Age of Viacom Users

112. Upon arriving on the Viacom Children's websites, Viacom encouraged its users to register and establish profiles for those websites.

⁴⁶ See http://blogs.msdn.com/b/jw_on_tech/archive/2012/03/13/why-i-left-google.aspx (last visited July 25, 2014).

⁴⁷ Viacom Exhibit D at 3.

⁴⁸ Though plaintiffs' investigation did not reveal the continued disclosure of information from Viacom to Google, plaintiffs' note that they have not had opportunity for discovery to determine whether disclosures between the defendants continue to occur that is not detectable from the plaintiffs' individual computers.

113. During the registration process, Viacom obtained the birthdate and gender of its users.

114. Correct Image of the Nick.com Sign-Up Process:

- a. In response to Plaintiffs' initial Consolidated Complaint Defendant Viacom filed Exhibit A, which included the following image as a purported representation of the sign-up process at Nick.com.

REGISTRATION CLOSE X

GET A NICKNAME:
Getting a NickName is **EASY, FREE** and **SAFE!** With a NickName, you can:

- Create your own Avatar, Profile, and Room!
- Play **EVERY** game on Nick.com!
- Keep track of your favorite videos and games!
- Access to the Club! Plus even **MORE!**

What are you waiting for?

HEY GROWN-UPS:
We don't collect **ANY** personal information about your kids. Which means we couldn't share it even if we wanted to! NickNames allows kids to take advantage of great features like NickPages, Message Boards and other ways kids can customize Nick.com.

NICKNAME/DISPLAY NAME
3 to 10 characters with **NO SPACES**. **DON'T** use your real name or any personal info.

PASSWORD
DON'T use your username, real name or any personal info, and keep it 3 to 10 characters with **NO SPACES**.

RETYPE PASSWORD
Retype your password to confirm (just to be sure.)

PASSWORD HINT
What was the name of your kindergarten teacher?

Answer:

GENDER
Why do we ask? So we can make Nick.com the best it can be for ALL of our fans.

☒ Male ☐ Female

CONFIRM
☒ I have read the [Privacy Policy/Tour California Privacy Rights and Terms of Use](#).

- b. Defendant Viacom misrepresented the sign-up process at Nick.com at the time in December 2012 when the plaintiff's filed suit. The Defendant's misrepresentation excludes the request for a minor child's exact birthdate. The correct version requires an exact birthdate for a child to create an account. This is a correct image of the Sign-Up process at the time Plaintiff's filed suit:

JOIN THE CLUB CLOSE X

GET A NICKNAME:
Getting a NickName is EASY, FREE and SAFE! With a NickName, you can:

- Create your own Avatar, Profile, and Room!
- Play EVERY game on Nick.com!
- Keep track of your favorite videos and games!
- Access to the Club! Plus even MORE!

What are you waiting for?

HEY GROWN-UPS:
We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to! NickNames allows kids to take advantage of great features like NickPages, Message Boards and other ways kids can customize Nick.com.

NICKNAME/DISPLAY NAME
3 to 30 characters with NO SPACES. DON'T use your real name or any personal info.

PASSWORD
DON'T use your username, real name or any personal info, and keep it 3 to 30 characters with NO SPACES.

RETYPE PASSWORD
Retype your password to confirm (Just to be sure.)

PASSWORD HINT
When's your birthday?

ANSWER:

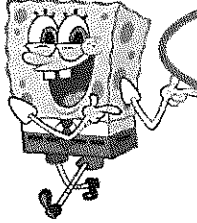
YOUR BIRTHDAY
This helps us make new stuff just for you, which helps make Nick.com even better! (Example: 11/05/1991)

Month Day Year

GENDER
Why do we ask? So we can make Nick.com the best it can be for ALL of our fans.

☐ Male ☐ Female

CONFIRM
☐ I have read the Privacy Policy/Your California Privacy Rights and Terms of Use.



115. Viacom gave its users an internal code name based upon their answers to the gender and birth date questions. For instance, Viacom gave 6 year-old males the code name “Dil”, and 12 year-old males the code name “Lou”. Viacom calls this coding mechanism the “rugrat” code.

116. When a child registered for an account, the child would also create a unique profile name that was tied to that child’s profile page.

117. Viacom associated each profile name with a first party identification cookie that had its own unique numeric or alphanumeric identifier.

118. Viacom disclosed to Google each child’s profile name.

119. Viacom also disclosed to Google the code name for the child’s specific gender and age.

120. Through these disclosures and the disclosure of the persistent cookie identifier of the DoubleClick.net cookie, and the Plaintiffs’ IP address, browser settings and other information explained above, Viacom knowingly disclosed to Google information which,

without more, when disclosed to Google, itself links the actual plaintiffs' to specific video materials for Defendant Google based on information that Google already has in its control.

L. How Viacom Disclosed the Plaintiff Minor Children's Video Viewing Histories

121. The Viacom children's websites offer children the ability to view and/or interact with video materials.

122. When a child viewed a video, or played a video game on a Viacom site, an online record of the activity was made.

123. Viacom provided Google with the online records disclosing its users' video viewing activities.

124. For instance, the following video viewing activity of a Nick.com user was provided to Google and stored within Google's doubleclick.net domain cookies:

`http://ad.doubleclick.net/adi/nick.nol/atf_i_s/club/clubhouses/penguins_of_madagascar_shorts_skippers_nightmare49;sec0=clbu;sec1=clubhouses;sec2=penguins_of_madagascar_shorts_skippers_nightmare;cat=2;rugrat=Dil50;lcategory=pom_teaser;show=pom_teaser;gametype=clubhouses;demo=D;site=nick;lcategory=nick;u=...[the user's unique third party cookie alphanumeric identifier appears at the end of the string])`

125. The online record Viacom provided to Google included the code name that specified the child's gender and age, which in the foregoing example is `rugrat=Dil`, denominating a male user, age 6. Viacom also disclosed each individual plaintiff's username to Google that was input when a child logged-in or visited his or her profile page, a process through which Google could use its unique numeric or alphanumeric identifier to associate the video materials watched by a specific child with the profile name and profile page of that specific child.

126. From this data, Google was able to compile a history of any particular child's

⁴⁹ *Penguins of Madagascar Skipper's Nightmare* is the name of the video requested by this user.

⁵⁰ "Dil" is the code name Viacom gives to male users, age 6.

video viewing activity.

127. At no point did Viacom or Google seek or receive the informed, written consent of any Plaintiff or their parent to disclose the video materials requested and obtained by the Plaintiffs from Viacom's children's websites to a third-party at the time such disclosure was sought and effectuated.

VI. CLASS ACTION ALLEGATIONS

128. This putative class action is brought pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3). The Plaintiffs bring this action on behalf of themselves and all similarly situated minor children under the age of 13 as representatives of a class and a subclass defined as follows:

U.S. Resident Class: All children under the age of 13 in the United States who visited the website Nick.com and had Internet cookies that tracked their Internet communications placed on their computing devices by Viacom and Google.

Video Subclass: All children under the age of 13 in the United States who were registered users of Nick.com and who engaged with one or more video materials on such site, and who had their video viewing histories knowingly disclosed by Viacom to Google.

129. Each Plaintiff meets the requirements of both the U.S. Resident Class and Video Subclass.

130. The particular members of the proposed Class and Subclass are capable of being described without managerial or administrative difficulties. The members of the Class and Subclass are readily identifiable from the information and records in the possession or control of the Defendants.

131. The members of the Class and Subclass are so numerous that individual joinder of all members is impractical. This allegation is based upon information and belief that Defendants intercepted the video-viewing histories and Internet communications of millions of Nick.com

users.

132. There are questions of law and fact common to the Class and Subclass that predominate over any questions affecting only individual members of the Class or Subclass, and, in fact, the wrongs suffered and remedies sought by the Plaintiffs and other members of the Class and Subclass are premised upon an unlawful scheme participated in by each of the Defendants.

The principal common issues include, but are not limited to, the following:

- a. Whether Viacom constitutes a video tape service provider as defined in the Video Privacy Protection Act;
- b. The nature and extent to which video materials requested and obtained by Viacom website users were disclosed in violation of the Video Privacy Protection Act;
- c. Whether the Defendants “intercepted” the electronic communications of members of the Class in violation of the Electronic Communications Privacy Act;
- d. Whether the Defendants utilized “devices” to intercept the online communications of the class;
- e. Whether the Defendants intercepted “content” as described in the Electronic Communications Privacy Act;
- f. Whether the Defendants intercepted the online communications of the Plaintiffs for a criminal or tortious purpose;
- g. Whether the actions taken by the Defendants violate the Stored Communications Act;
- h. Whether the Defendants accessed a “facility” as described in the Stored

Communications Act;

- i. Whether the Defendants accessed a facility without authorization as described in the Stored Communications Act;
- j. Whether the actions taken by the Defendants violate the Computer Fraud and Abuse Act;
- k. Whether the actions taken by the Defendants violate the California Invasion of Privacy Act;
- l. Whether the actions taken by the Defendants violate the New Jersey Computer Related Offenses Act;
- m. Whether or not Viacom should be enjoined from further disclosing information about the video materials its minor children users watch on its sites, and whether Google should be enjoined from further accessing such information without the proper consent of Plaintiffs;
- n. Whether or not the Defendants should be enjoined from further intercepting any electronic communications without the proper consent of the Plaintiffs;
- o. Whether the Defendants intruded upon the Plaintiffs' seclusion;
- p. Whether the Plaintiffs are entitled to recover profits gained at their expense by the Defendants under a claim for unjust enrichment;
- q. The nature and extent of all statutory penalties or damages for which the Defendants are liable to the Class and Subclass members; and
- r. Whether punitive damages are appropriate.

133. The common issues predominate over any individualized issues such that the

putative class is sufficient cohesive to warrant adjudication by representation.

134. The Plaintiffs' claims are typical of those of the members of the Class and Subclass and are based on the same legal and factual theories.

135. Class treatment is superior in that the fairness and efficiency of class procedure in this action significantly outweighs any alternative methods of adjudication. In the absence of class treatment, duplicative evidence of Defendant's alleged violations would have to be provided in thousands of individual lawsuits. Moreover, class certification would further the policy underlying Rule 23 by aggregating class members possessing relatively small individual claims, thus overcoming the problem that small recoveries do not incentivize plaintiffs to sue individually.

136. The Plaintiffs, by and through their Next Friends, will fairly and adequately represent and protect the interests of the members of the Class. The Plaintiffs have suffered injury in their own capacity from the practices complained of and are ready, willing, and able to serve as Class representatives. Moreover, Plaintiffs' counsel is experienced in handling class actions and actions involving unlawful commercial practices, including such unlawful practices on the Internet. Neither the Plaintiffs nor their counsel has any interest that might cause them not to vigorously pursue this action. The Plaintiffs' interests coincide with, and are not antagonistic to, those of the Class members they seek to represent.

137. Certification of a class under Federal Rule of Civil Procedure 23(b)(2) is appropriate because the Defendants have acted on grounds that apply generally to the Class such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

138. Certification of a class under Federal Rule of Civil Procedure 23(b)(3) is appropriate in that the Plaintiffs and the Class Members seek monetary damages, common

questions predominate over any individual questions, and a plaintiff class action is superior for the fair and efficient adjudication of this controversy. A plaintiff class action will cause an orderly and expeditious administration of Class members' claims and economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured. Moreover, the individual members of the Class are likely to be unaware of their rights and not in a position (either financially or through experience) to commence individual litigation against these Defendants.

139. Alternatively, certification of a plaintiff class under Federal Rule of Civil Procedure 23(b)(1) is appropriate in that inconsistent or varying adjudications with respect to individual members of the Class would establish incompatible standards of conduct for the Defendants or adjudications with respect to individual members of the Class as a practical matter would be dispositive of the interests of the other members not parties to the adjudication or would substantially impair or impede their ability to protect their interests.

COUNT I – VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT

Children's Video Subclass v. All Defendants

140. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

141. The Video Privacy Protection Act, 18 U.S.C. § 2710, (hereinafter "VPPA"), prohibits a video tape service provider from knowingly disclosing personally identifiable information concerning any consumer of such provider to a third-party without the informed written consent of the consumer given at the time such disclosure is sought.

- a. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar

audiovisual materials.”

- b. As defined in 18 U.S.C. § 2710(a)(3), “personally identifiable information” is open-ended and “includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.”
- c. As defined in U.S.C. § 2710(a)(1) a “consumer” means “any renter, purchaser or subscriber of goods or services from a video tape service provider.”
- d. There is no exception in the VPPA for disclosures to a third-party which publicly promises not to use personally identifiable information.
- e. As specified in 18 U.S.C. § 2710(b)(2)(B) at the time this action was filed, valid consent under the VPPA is the “informed, written consent of the consumer given at the time the disclosure is sought.”⁵¹

142. As amended in December 2012, the VPPA creates an opt-out right for consumers. It requires VTSPs that disclose personally identifiable information with the “informed, written consent” of the consumer to also “provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer’s election.” 18

⁵¹ After years of lobbying by online video service providers, Congress amended the “consent” portion of the VPPA. This action was brought under this previous definition of “consent.” The new definition, also found in 18 U.S.C. § 2710 (b)(2)(B) provides that consent must be “informed, written consent (including through an electronic means using the Internet of the consumer that – (i) is in a form distinct and separate from an form setting forth other legal or financial obligations of the consumer; (ii) at the election of the consumer—(I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer’s election.”

U.S.C. § 2710(2)(B)(iii).

143. The Video Privacy Protection Act of 1988 was passed for the explicit purpose of protecting the privacy of individuals' and their families' video requests and viewing histories. As explained in the Senate report for the Act, "The impetus for this legislation occurred when a weekly newspaper in Washington published a profile of Robert H. Bork based on the titles of 146 files *his family had rented* from a video store." S. Rep. 100-599 at 6 (1988).

144. At the time of its passage, Congress was well aware of the impact of ever-changing computer technology. Upon the VPPA's introduction, the late Senator Paul Simon noted:

There is no denying that the computer age has revolutionized the world. Over the past 20 years we have seen remarkable changes in the way each of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before. Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.

S. Rep. No. 100-599 at 7-8 (1988) (emphasis added).

145. Senator Patrick Leahy also remarked at the time that new privacy protections were needed:

It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs

they watch, who are some of the people they telephone I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

S. Rep. No. 100-599 at 5-6 (1988).

146. Sen. Leahy later explained:

It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not anybody else's business, whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business."⁵²

147. The sponsor of Act, Rep. Al McCandless, also explained:

There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of intellectual thought. The whole process of intellectual growth is one of privacy – of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

S. Rep. No. 100-599 at 7.

148. The legislative history of the VPPA proves that Congress understood that technology would soon make tracking “relatively easy” and the intent of the VPPA was to keep up with technology. Congress understands how to define a statutory term in a manner that makes it closed to future real-world development. With the VPPA, however, Congress chose to define “personally identifiable information” in a way that allowed it to be applied to changes in technology. The legislative history to the 1988 Act makes clear, “Unlike the other definitions in [the VPPA], paragraph (a)(3) uses the word ‘includes’ to establish a minimum, but not exclusive,

⁵² GPO.gov, House Report 112-312, December 2, 2011, <http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt312/html/CRPT-112hrp312.htm> (last visited September 16, 2013).

definition of personally identifiable information.” S. Rep. 100-599 at 12 (1988).

149. Congress recognized the definition of PII for children’s use of the Internet in the legislative history to the 2012 amendments:

This Committee does not intend for this clarification to negate in any way existing laws, regulations, and practices designed to protect the privacy of children on the Internet. ...

Website operators ... share in the responsibility to protect consumer privacy, particularly the privacy of children. To facilitate this goal, Congress enacted the Children’s Online Privacy Protection Act effective April 21, 2000, which applies to the online collection of personal information from children under 13. Compliance with the Act is overseen by the Federal Trade Commission, which enacted rules governing web site operator compliance, including a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children’s privacy and safety online.

...

The Act and its regulations apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information – for example, hobbies, interests, and information collected through cookies and other types of tracking mechanisms – when they are tied to individually identifiable information.

H. Rep. 112-312 at 3-4 (2011).

150. The information at issue in this case fits the current real-world definition of “personally identifiable information.” For example:

- a. For its websites targeted to adults, Defendant Viacom defines “Personal Information” as “information that would allow someone to identify you or contact you[.]” It then provides examples, “such as your full name, email address or telephone number.”⁵³

⁵³ See <http://www.vh1.com/interact/terms/privacy.jhtml> (last visited July 29, 2014).

- b. IP addresses, unique device identifiers, persistent cookie identifiers, browser-fingerprints, and usernames/aliases can all be used to identify or contact a person – particularly when the entity to which such information is disclosed is the world’s largest Internet company and tracks user real names, addresses, geo-locations, phone numbers, contacts, and behavior across a suite of the world’s most popular Internet services.
- c. For adults, the data tracking industry defines “PII” to “include[] the following information about a specific individual: name, address, telephone number, and email address – when used to identify a particular individual. Data is not considered PII under the Principles if the data is not used in an identifiable manner. For example, in situations where an IP address is not linked with other PII, the IP address itself would not in most instances be PII for purposes of these Principles. In instances, where an IP address is in fact linked to an individual in its collection and use, in most instances the IP address would be PII for purposes of these Principles. A similar analysis would apply for other persistent identifiers such as a customer number held in a cookie or processor serial number. When such identifier is in fact coupled with an individual identifier within the definition of PII, such as first and last name, such information would be PII for purposes of the Principles. When such data is not coupled with an individual identifier within the PII definition, the data would not be PII.”⁵⁴
- d. Both Defendants Viacom and Google are members of the Interactive

⁵⁴ Self-Regulatory Principles for Online Behavioral Advertising at 25, July 2009. Available at: <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> (last visited July 30, 2014).

Advertising Bureau and agree to comply with the IAB's Code of Conduct. In particular, Viacom and Google publicly promise through IAB membership that they will "not collect 'personal information' as defined in the Children's Online Privacy Protection Act ('COPPA'), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising direct to children they have actual knowledge are under the age of 13 except as compliant with the COPPA."

- e. For children, the data tracking industry defines "personal information" as it is defined in the Children's Online Privacy Protection Act where the tracking company "has actual knowledge" that the child is under the age of 13 or where the tracking is done on a website direct to children under the age of 13.⁵⁵
- f. The Federal Trade Commission, after extensive hearings, and in its fact-finding role regarding regulation of children's use of the Internet, found that persistent identifiers are PII:

The Commission continues to believe that persistent identifiers permit the online contacting of a specific individual. As the Commission stated in the 2011 NPRM, it is not persuaded by arguments that persistent identifiers only permit the contacting of a device. This interpretation ignores the reality that, at any given moment, a specific individual is using that device. Indeed, the whole premise underlying behavioral advertising is to serve an advertisement based on the perceived preferences of the individual user.

Nor is the commission swayed by arguments noting that multiple

⁵⁵ Id. at 16-17.

individuals could be using the same device. Multiple people often share the same phone number, the same home address, and the same email address, yet Congress still classified those, standing alone, as "individually identifiable information about an individual." For these reasons, and the reasons stated in the 2011 NRPM, the Commission will retain persistent identifiers within the definition of personal information.

g. Under COPPA, the FTC defines "personal information" as follows:

Personal information means individually identifiable information about an individual collected online, including:

- (1) A first and last name;
- (2) A home or other physical address including street name of a city or town;
- (3) Online contact information as defined in this section;⁵⁶
- (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;
- (5) A telephone number;
- (6) A Social Security number;
- (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;
- (8) A photograph, video, or audio file where such file contains a child's image or voice;
- (9) Geolocation information sufficient to identify street name and name of a city or town; or
- (10) Information concerning the child or parents of the child that the operator⁵⁷ collects online from the child and combines with an identifier described in this definition.

h. The Gramm-Leach Financial Modernization Act of 1999 prohibits

⁵⁶ "Online contact information" is defined as "an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over Internet protocol (VOIP) identifier, or a video chat user identifier. 16 C.F.R. § 312.2

⁵⁷ Both Defendants are "operators" under the FTC's definition, "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users or visitors to such Web site or online service." 16 C.F.R. § 312.2

financial institutions from directly or indirectly “disclos[ing] to a nonaffiliated third party any non public personal information” of a consumer. 15 U.S.C. § 6802. Like the VPPA, the Gramm-Leach Act defined “nonpublic personal information” in an open-ended fashion, as “personally identifiable financial information” provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by a financial institution. 15 U.S.C. § 6802(4). Charged with implementing this statute, the Securities Exchange Commission has found that “personally identifiable financial information includes: ... any information [collected] through an Internet ‘cookie’ (an information collecting device from a web server.” 17 C.F.R. § 248.3.

- i. The Federal Education Rights and Privacy Act (FERPA) provides that no federal funds shall be made available to any educational agency which has a policy or practice of permitting the release of education records or “personally identifiable information contained therein other than directory information” without the written consent of their parents to any third party (with exceptions). 20 U.S.C. § 1232g(b)(1). Charged with implementing this same open-ended statutory phrase of “personally identifiable information,” the United States of Department of Education has found that “personally identifiable information” is a term which “includes, but is not limited to (a) the student’s name; (b) the name of the student’s parent or other family members; (c) the address of the student or student’s family;

(d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty, or (g) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates." 34 C.F.R. § 99.3.

- j. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects "individually identifiable health information" which the statute defines to include "any information, including demographic information collected from an individual that" is created by a covered entity, relates to their health and "identifies the individual" or "with respect to which there is a reasonable basis to believe the information can be used to identify the individual." In implementing HIPAA, the United States Department of Health and Human Services has found that the following types of information are "direct identifiers" of individuals: (i) names; (ii) addresses, (iii) phone numbers; (iv) fax numbers; (v) email addresses; (vi) Social Security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license

plate numbers; (xii) device identifiers and serial numbers; (xiii) URLs; (xiv) IP addresses; (xv) biometric identifiers, including finger and voice prints, and (xvi) full face photographic images and any comparable images.” 45 C.F.R. § 164.514(2).

- k. The Privacy Act, which protects Americans’ information held by federal government agencies, has also been interpreted to protect persistent identifiers as personally-identifiable information. In particular, the statute protects “records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” 5 U.S.C. § 552a(5). For its own purposes in protecting Americans’ privacy, the federal government defines PII as “any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.”⁵⁸ In 2011, the federal government clarified that the definition of PII “is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific

⁵⁸ OMB Memorandum M-07-16, “Memorandum for Chief Information Officers” from OMB Office of E-Government and Information Technology, July 12, 2006. Available at: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf> (last visited July 30, 2014).

risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.”⁵⁹

151. Online video service providers were well-aware of the restrictions imposed by the VPPA. For instance, in 2012, online video service provider Netflix lobbied for legislation to amend the Act to no longer require consent every time it sought to disclose a video requested or viewed by a customer.

152. As stated clearly in the legislative history to the VPPA amendments of 2012:

Since 1988, Federal law has authorized video tape service providers to share customer information with the ‘informed, written consent of the consumer at the time the disclosure is sought.’ This consent must be obtained each time the provider wishes to disclose.

House Report 112-312 at 4. (2011).

153. The VPPA also clearly applies to online VTSPs that show television shows. As explained in the legislative history of the 2012 amendments:

When this law was originally enacted in 1988, consumers rented movies from brick-and-mortar video stores such as Blockbuster. Today, not only are VHS tapes obsolete, so too are traditional video rental stores. The Internet has revolutionized how consumers rent and watch movies and television programs. Video stores have been replaced with “on-demand” cable services or Internet streaming services that allow a customer to watch a movie or TV show from their laptop or even their cell phone.

House Report 112-312 at 2. (2011).

⁵⁹ OMB Memorandum M-10-22, “Guidance for Online Use of Web Measurement and Customization Technologies,” June 25, 2010. Available at: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf (last visited July 30, 2014).

At the time of the VPPA's enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988 – the VHS cassette tape – is no obsolete. In its place, the Internet has revolutionized the way that American consumers rent and watch movies and television programs. Today, so-called “on-demand” cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.

S. Rep. 112-258 at 2 (2012)

154. Viacom is engaged in the business of the delivery of pre-recorded video cassette tapes or similar audio visual materials as defined by the VPPA in that the home page of Nick.com advertises it as the place to watch “2000+ FREE ONLINE VIDEOS and “play “1000+ FREE ONLINE GAMES.” The homepage prominently features a rotating section enticing users to click and watch various videos with action buttons that say “Watch now,” “Check it out,” or, in the case of games, “Play Now.” In addition, two of the first three links in the top bar on the homepage refer to audio-visual materials. *See* Nick.com (last visited September 24, 2013).

155. Plaintiffs and members of the putative video sub-class are “consumers” under the VPPA in that they are registered users of Nick.com and, therefore, constitute subscribers to the video services Viacom provides on Nick.com.

156. Viacom disclosed to Google at least the following about each Plaintiff who was a registered user of Viacom's children's websites: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites, and (11) the DoubleClick persistent cookie identifier.

157. By disclosing the above information to Google, Viacom knowingly disclosed information which, without more, when disclosed to Google, links specific persons with their

video requests and/or viewing histories based on information that Google already has in its possession.

158. Viacom violated the VPPA by knowingly disclosing to Google information which, without more, when disclosed to Google, links specific persons with their video requests and viewing histories based on information that Google already has in its possession.

159. Google violated the VPPA by knowingly obtaining Plaintiffs' personally identifiable information in the form of the specific video materials and services requested and obtained by Plaintiffs from Viacom.⁶⁰

160. Defendant Google knowingly accepted the Plaintiffs' personally identifiable information regarding video materials and services through its use of the doubleclick.net cookies and other computer technologies.

161. Viacom further violated the VPPA after passage of the amended VPPA by failing to provide plaintiffs' with the opt-out right codified in the amended VPPA in 18 U.S.C. § 2710(2)(B)(iii).

162. As a result of the above violations and pursuant to 18 U.S.C. § 2710, the Defendants are liable to the Plaintiffs and the Class for "liquidated damages of not less than \$2,500 per plaintiff; reasonable attorney's fees and other litigation costs; injunctive and declaratory relief; and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future."

⁶⁰ Plaintiffs' recognize this Court's previous Order only permitted leave to amend their VPPA claim against Defendant Viacom. Plaintiff's repeat their claim against Google herein to make clear that they have not abandoned such claim for purposes of a potential appeal.

COUNT II – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

U.S. Resident Children v. All Defendants

163. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

164. Enacted in 1986, the Electronic Communications Privacy Act (“ECPA”) amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. The ECPA prohibits the unauthorized interception of the contents of electronic transmissions such as those made by Plaintiffs in this case.

165. Representative Kastenmeier discussed the scope the ECPA amendments were designed to reach:

“ . . . [L]egislation which protects electronic communications from interceptions...should be comprehensive, and *not limited to particular types or techniques of communicating* Any attempt to . . . protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years....what is being protected is *the sanctity and privacy of the communication*. We should not attempt to discriminate for or against certain methods of communication”⁶¹

166. Moreover, Senator Leahy discussed the purpose of the ECPA:

“Today Americans have at their fingertips a broad array of telecommunications and computer technology, including . . . *computer-to-computer links* When title III was written 18 years ago, Congress could barely contemplate forms of telecommunications and computer technology we are starting to take for granted today Senate bill 2575...is designed to . . . provide a reasonable level of Federal privacy protection to these new forms of communication.”⁶²

167. As described herein, Google intentionally intercepted the contents of electronic communications of minor children under the age of 13 who visited Nick.com, through Google’s

⁶¹ 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Rep. Kastenmeier) (emphasis added).

⁶² 132 Cong. Rec. S14441-04 (1986) 1986 WL 786307 (comments from Sen. Leahy) (emphasis added).

use of devices that tracked and recorded the Plaintiffs' web communications, including but not limited to their Internet browsing histories and without consent.

168. Google's DoubleClick.net cookies tracked at least the following information regarding each individual Plaintiff: (1) unique IP address; (2) browser setting; (3) unique device identifier; (4) operating system; (5) screen resolution; (6) browser version; (7) and web communications, including but not limited to detailed and unique URL requests (which included video materials requested and obtained from Viacom's children's websites).

169. The specific Uniform Resource Locators the Plaintiffs typed into and sent through their web browsers are "contents" within the meaning of the ECPA because they include "any information concerning the substance, purport, or meaning of that communication" as defined in 18 U.S.C. § 2510 (8).

170. Google's tracking and interceptions began immediately upon the Plaintiffs' first communications with Defendant Viacom's children's websites and before any consent could be obtained from the Plaintiffs' and Class Members' guardians.

171. Google's cookies tracked and recorded the content of the web communications of the Plaintiffs and class members contemporaneous to, and, in some cases, before the Plaintiffs' communications with other websites were consummated such that the tracking and recording was contemporaneous with the Plaintiffs' communications and while the communications were in transit.

172. After Plaintiffs registered with the Viacom site, Google also accessed their individual username, gender, and birthdate.

173. Defendant Google's doubleclick.net "id", cookies:

- a. Were placed on Plaintiffs' computing devices before each Plaintiff created

an account or logged-in to the respective Viacom children's websites.

- b. Remained on the Plaintiffs' computing devices even after individual users who were minor children under the age of 13 had created an account or logged-in and informed Viacom that they were minor children under the age of 13.
- c. Are capable of determining each individual user's response to Viacom's "birthdate" question in the form which was necessary to create a user account and collects information about the user's age via computer code.

174. The transmission of data between the Plaintiffs' computing devices and Viacom's children's websites and other non-Viacom websites hosted by servers are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

175. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5).

- a. Each individual cookie that Google used to track the Plaintiffs' communications;
- b. The Plaintiffs' browsers which Google used to place and extract data from each Defendant's individual cookies;
- c. The Plaintiffs' computing devices;
- d. Each Defendant's web server;
- e. The plan Google carried out to effectuate its purpose of tracking the electronic communications of minor children.

176. The Plaintiffs, minor children under the age of 13, did not, and as a matter of law could not have, consented to the tracking of their web usage and communications.

177. The Plaintiffs' legal guardians did not consent to the tracking of Plaintiffs' web

usage and communications.

178. Viacom, as a matter of law, could not have consented to the tracking of the web usage and communications of minor children under the age of 13 using their websites without the consent of their guardians.

179. The Defendants' actions were done for the tortious purpose of intruding upon the Plaintiffs' seclusion as set forth in this Complaint.

180. The Defendants' actions were done for criminal purposes in violation of numerous federal and state statutes, including, but not limited to 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act.

181. Upon information and belief, in addition to intercepting the Plaintiffs' communications with the Viacom children's websites, Google used the cookies to track the Plaintiffs' communications with other websites on which Google places advertisements and related tracking cookies despite Google's knowledge that the Plaintiffs were minor children and without the consent of the Plaintiffs, their guardians, or the other websites with which the Plaintiffs were communicating.

182. Viacom procured Google to intercept the content of Plaintiffs' Internet communications with other websites. Upon information and belief, Viacom profited from Google's unauthorized tracking of the Plaintiffs' Internet communications with other websites as such information assisted in the sale of targeted advertisements to children on the Viacom sites.

183. Viacom knew or had reason to know that Google intentionally intercepted the content of the Internet communications of the Plaintiffs on non-Viacom websites with tracking cookies deposited and/or accessed on Viacom's websites despite Google's knowledge that the Plaintiffs were minor children and that it did not have either the Plaintiffs' or their guardians'

consent to intercept their Internet communications.

184. As a direct and proximate cause of such unlawful conduct, the Defendants violated the ECPA in that they:

- a. Intentionally intercepted or procured another person to intercept the contents of wire and/or electronic communications of the Plaintiffs.
- b. Upon belief predicated upon further discovery, intentionally disclosed to another person the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and
- c. Upon belief predicated upon further discovery, intentionally used or endeavored to use the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a).

185. As a result of the above violations, and pursuant to 18 U.S.C. § 2520, the Defendants are liable to the Plaintiffs and the Class in the sum of statutory damages consisting of the greater of \$100 for each day each of the class members' data was wrongfully obtained or \$10,000 per violation, whichever is greater; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future, and reasonable attorney's fees and other litigation costs.

COUNT III – THE STORED COMMUNICATIONS ACT

U.S. Resident Children v. Google

186. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

187. The Stored Communications Act (hereinafter “SCA”) provides a cause of action against any person who “intentionally accesses without authorization a facility through which an electronic communication service is provided,” or any person “who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system.” 18 U.S.C. § 2701(a).

188. The SCA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

189. The SCA defines an “electronic communications service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

190. Defendants intentionally accessed without authorization or intentionally exceeded authorization to access facilities through which an electronic communications services was provided when they used the instrumentalities described in this Complaint to access the Plaintiffs’ web-browsers and computing devices for purposes of tracking the Plaintiffs’ Internet communications.

191. The web browsers utilized by the Plaintiffs on their computing devices provide electronic communications services to the Plaintiffs because they “provide to users thereof the

ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

192. The Internet Service Providers to which the Plaintiffs use or subscribe to provide electronic communication services to the Plaintiffs because they “provide to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

193. Neither the Plaintiffs’ browsers nor the Internet Service Providers authorized the extent of the Defendants’ access to the Plaintiffs’ computing devices.

194. The Plaintiffs’ respective web browsers store cookie and other information in browser-managed files on the Plaintiffs’ computing devices. These browsers are also facilities under the SCA because they comprise the software necessary for and “through which (the) electronic communications service is provided.”

195. Google intentionally accessed Plaintiffs’ web browsers without authorization when Google accessed Plaintiffs’ browsers immediately upon the Plaintiffs’ visiting Viacom’s children’s websites and after sign-up without obtaining the consent of the Plaintiffs or their guardians.

196. The Plaintiffs’ computing devices are facilities under the SCA because they comprise the hardware necessary for and “through which (the) electronic communications service is provided.”

197. The cookies in the browser-managed files that Plaintiffs’ web browsers store are updated regularly to record users’ browsing activities and communications as they happen. For that reason, when Google accesses these facilities to acquire Plaintiffs’ electronic communications, it acquires profile information and related just-transmitted electronic communications out of random access memory (“RAM”). Google acquires the profile information and related electronic communications out of electronic storage, incidental to the

transmission thereof.

198. Upon information and belief, the acquisition of electronic communications from the Plaintiffs' web browsers and computing devices included the contents of communications the Plaintiffs had with non-Viacom websites that are not affiliated with Google.

199. Plaintiffs and Class Members were harmed by Defendant's violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendants attributable to the violations or statutory minimum damages of \$1,000 per person, punitive damages, costs, and reasonable attorney's fees.

COUNT IV – THE COMPUTER FRAUD AND ABUSE ACT

U.S. Resident Children v. All Defendants

200. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

201. The Computer Fraud and Abuse Act, codified at 18 U.S.C. Sec. 1030 et seq., prohibits the unauthorized access of a computer or computing device.

202. The Plaintiffs' and Class Members' computing devices were used in interstate commerce or communication in that Plaintiffs' use of the Viacom's children's websites and other websites involved Internet communications across state lines.

203. Google intentionally accessed without authorization or intentionally exceeded authorized access to the Plaintiffs' computing devices when it placed and accessed third-party cookies on the Plaintiffs' computing devices to track the Plaintiffs' communications on Viacom's children's websites and other websites across the Internet.

204. Google's unauthorized access started immediately upon the Plaintiffs' first communication with the Viacom children's websites and continued without authorization from the Plaintiffs' guardians.

205. The Plaintiffs' and Class Members' computing devices are protected computers as defined in 18 U.S.C. § 1030(e)(2).

206. Google used its intentional unauthorized access to obtain information from the Plaintiffs' and Class Members' computing devices, such as third-party cookie data stored there, in violation of 18 U.S.C. § 1030(a)(2)(c).

207. Defendant Viacom violated 18 U.S.C. § 1030(b) when it permitted, acquiesced to, facilitated, and participated in the activity alleged herein by serving as the conduit through which Google gained illegal access to the Plaintiffs' computing devices.

208. Upon information and belief, Viacom then profited from Google's unauthorized access to the plaintiff's computing devices through the sale of targeted advertisements to Plaintiffs on Viacom's children's websites.

209. Google knowingly caused the transmission of a program, information, code, or command and as a result intentionally caused a loss to Plaintiffs and Class Members during a one-year period aggregating at least \$5,000 in value, in violation of 18 U.S.C. § 1030(a)(5)(a)(i).

210. Google intentionally accessed Plaintiffs' and Class Members' computing devices without authorization or exceeded authorized access and as a result caused a loss to Plaintiffs and Class Members during a one-year period aggregating at least \$5,000 in value, in violation of 18 U.S.C. § 1030(a)(5)(a)(iii).

211. The Defendants' unlawful access to Plaintiffs' and Class Members' computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendants may continue to commit such acts. Plaintiffs' and Class Members' remedies at law are not adequate to compensate for these inflicted and threatened injuries, entitling Plaintiffs and the Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT V – THE CALIFORNIA INVASION OF PRIVACY ACT

U.S. Resident Children v. All Defendants

212. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

213. California Penal Code § 631(a) provides, in pertinent part:

Any person who . . . willfully and without the consent of *all* parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars

(emphasis added)

214. The Defendants' tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications, including web-browsing and video-viewing histories, was done without authorization or consent of either the Plaintiffs and Class Members or their guardians.

215. Google's corporate headquarters are located in California.

216. On information and belief, a substantial portion of the putative class and plaintiff L.G. reside in the State of California and accessed the Viacom Children's websites from computing devices in the state of California.

217. Upon information and belief, Google directed and used the tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications in the state of California.

218. As a result of Google's actions in California, every act of tracking and every interception of the Plaintiffs' and Class Members' personal information and Internet

communications took place, in part, in California, regardless of the location of each individual Plaintiff and Class Member.

219. Plaintiffs and Class Members did not consent to any of the third-party tracker Defendants' actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

220. Plaintiffs and Class Members, as a matter of law, could not have consented to Google's actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

221. Viacom aided, conspired with, and permitted Google to violate California Penal Code § 631(a) when Viacom permitted, acquiesced to, facilitated, and participated in the activity alleged herein by knowingly serving as the conduit through which Google placed its devices in positions to intercept the content of Plaintiffs' Internet communications. Viacom then profited from Google's interceptions through the sale of targeted advertisements to Plaintiffs on Viacom's children's websites.

222. Plaintiffs and Class Members have suffered loss by reason of these violations including, but not limited to, violation of their rights of privacy and loss of value in their Personally Identifiable Information.

223. Unless restrained and enjoined, the Defendants will continue to commit such acts.

224. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and the Class Members have been injured by the violations of Cal. Penal Code § 631, and each seek damages for the greater of \$5,000 or three times the amount of actual damages, whichever is greater, as well as injunctive relief.

COUNT VI – NEW JERSEY COMPUTER RELATED OFFENSES ACT

U.S. Resident Children v. All Defendants

225. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

226. N.J.S.A. 2A:38A-3 states that a person or enterprise is liable for:

- a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;
- b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;
- c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;
- d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or
- e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

227. Defendants did purposefully, knowingly and/or recklessly, without Plaintiffs', Class Members' or their respective guardians' authorization, access, attempt to access, tamper with, alter, damage, take, destroy, obtain and/or intercept Plaintiffs' and Class Members' computer, computer software, data, database, computer program, computer system, computer

equipment and/or computer network in violation of N.J.S.A. 2A:38A-1 et seq.

228. Specifically, Defendants accessed Plaintiffs' and Class Members' computers in order to illegally harvest Plaintiffs' and Class Members' personal information. Through conversion and without consent, Defendants harvested Plaintiffs' personal information for their unjust enrichment and to the financial detriment of Plaintiffs and Class Members. Had Plaintiffs, Class Members, and/or their parents and/or guardians known that Defendants were converting Plaintiffs' personal information for financial gain, Plaintiffs, Class Members, and/or their parents and/or guardians would have at least expected remuneration for their personal information at the time it was conveyed.

229. Furthermore, Defendants' unauthorized placement of cookies on Plaintiffs' and Class Members' computers caused digital damage to their computers which may require Plaintiffs' and/or Class Members' to spend money and/or time to remove the malicious cookies at issue.

230. Many of the computers that were accessed, the terminal used in the accessing, and/or the actual damages took place in New Jersey.

231. Plaintiffs CAF, CTF, MP and TP all reside in the State of New Jersey and accessed the Viacom Children's sites from computing devices within the State of New Jersey.

232. Pursuant to N.J.S.A. 2A:38A-1 et seq., Plaintiffs and the Class Members have been injured by the violations of N.J.S.A. 2A:38A-1 et seq., and each seek damages for compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation, as well as injunctive relief.

COUNT VII – INTRUSION UPON SECLUSION

U.S. Resident Children v. All Defendants

233. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

234. In carrying out the scheme to track the Plaintiffs' Internet communications as described herein without the consent of the Plaintiffs or their legal guardians, the Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion in that the Defendants took information from the privacy of the Plaintiffs' homes.

235. The Plaintiffs, minor children, did not, and by law could not, consent to the Defendants' intrusion.

236. The Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion is highly offensive to a reasonable person in that Defendants' conduct alleged above violated federal statutes designed to protect individual privacy. Specifically, the defendant's conduct violated the Wiretap Act because they engaged in a scheme to intentionally intercept the contents of the minor plaintiffs' electronic communications without their or their guardians' consent. In the alternative, should this Court find that Defendants' conduct did not violate the Wiretap Act, then this Court must find that the Defendants conduct violated the Pen Register Act, 18 U.S.C. 3121, et seq., which makes it a federal crime for any person to "install or use a pen register or trap and trace device" without the consent of the user of an electronic communication service. A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3). A "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. §

3127(4). Violation of the Pen Register Act is subject to imprisonment for one year.

237. By knowingly placing or facilitating the placing of third-party cookies on the computing devices of minor children who were not aware of and could not consent to their placement, the Defendants intentionally exceeded authorized access to the plaintiffs' computers and obtained information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and the corresponding computer crime statutes of all 50 states.

238. Defendants' actions in committing criminal acts violating the privacy rights of millions of American children is highly offensive to a reasonable person.⁶³

239. The Defendants' intentional intrusion on the Plaintiffs' solitude and seclusion is highly offensive to a reason person in that Defendants' conduct violated the Terms of Use of both the Internet Service Providers and the web-browsers employed by the Plaintiffs which prohibit the use of those services in criminal activity, unlawful activity, and the tracking of Internet communications without consent.

240. In December 2012, the same month plaintiffs initially filed their respective suits, the Center for Digital Democracy survey more than 2,000 adults about basic principles of children's online privacy.⁶⁴ When asked whether they agreed or disagreed with the following statements, the polled adults responded as follows:

- a. "It is wrong for advertisers to collect and keep information about where a

⁶³ *U.S. v. White*, 401 US 745, 767-8 (1971) ("In my view, the invasion of privacy of communications is a highly offensive practice which should be engaged in only where the national security is at stake.") (Quoting Lyndon B. Johnson) (J. Douglas dissenting).

⁶⁴ The survey is available at <http://www.centerfordigitaldemocracy.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf> (last visited July 25, 2014).

child goes online and what that child does online.”

- 45 percent strongly agree
- 13 percent somewhat agree
- 12 percent somewhat disagree
- 27 percent strongly disagree
- 3 percent do not know or refused to answer

b. “It is okay for advertisers to track and keep a record of a child’s behavior online if they give the child free content.”

- 5 percent strongly agree
- 6 percent somewhat agree
- 16 percent somewhat disagree
- 70 percent strongly disagree
- 3 percent do not know or refused to answer

c. “As long as advertisers don’t know a child’s name and address, it is okay for them to collect and use information about the child’s activity online.”

- 4 percent strongly agree
- 14 percent somewhat agree
- 13 percent somewhat disagree
- 67 percent strongly disagree
- 2 percent do not know or refused to answer

d. “Before advertisers put tracking software on a child’s computer, advertisers should receive the parent’s permission.”

- 82 percent strongly agree
- 9 percent somewhat agree
- 2 percent somewhat disagree
- 4 percent strongly disagree
- 2 percent don’t know or refused to answer

e. When asked, “There is a federal law that says that online sites and companies need to ask parents’ permission before they collect personal information from children under age 13. Do you think the law is a good idea or a bad idea?” 90 percent said it was a good idea, 7 percent said it

was a bad idea, and 2 percent did not know or refused to answer.

f. Parents in the survey were more protective of children's privacy than non-parents.

g. In connection with an investigation of cookie tracking on children's websites, the Wall Street Journal asked readers:

How concerned are you about advertisers and companies tracking your behavior across the web?" An overwhelming majority of respondents indicated concern.

- 59.7 percent said they were "very alarmed"
- 25 percent said they were "somewhat alarmed"
- 3.7 percent said they were "neutral"
- 7 percent said it was "not a big worry"
- 4.5 percent said they "could not care less"⁶⁵

h. In November 2012, the Washington Post asked Americans:⁶⁶

How concerned are you, if at all, about the government or private companies collecting digital information from your computer or phone?

- 43 percent were "very concerned"
- 26 percent were "somewhat concerned"
- 18 percent were "not too concerned"
- 12 percent were "not at all concerned," and
- 1 percent had "no opinion"

How concerned are you, if at all, about the collection and use of your personal information by websites like Google, Amazon, or Ebay?

- 37 percent were "very concerned"
- 32 percent were "somewhat concerned"
- 17 percent were "not too concerned"

⁶⁵ See <http://blogs.wsj.com/wtk-kids/> (last visited July 30, 2014).

⁶⁶ See http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/12/21/National-Politics/Polling/question_12669.xml?uuid=FuyJGmqMEeOZe5ITsX2slw (last visited July 30, 2014).

- 13 percent were “not at all concerned”
- 2 percent had “no opinion”

i. In Winter 2012, the Pew Research Center on the Internet and American

Life asked Americans:

Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online – even if neither is exactly right?

- 68 percent said, “I’m not okay with it because I don’t like having my online behavior tracked and analyzed.”
- 28 percent said, “I’m okay with it because it means I see ads and get information about things I’m really interested in.”
- 4 percent said “neither” or “don’t know.”

241. Scope Matters – Defendants’ actions were highly offensive to reasonable people for each plaintiff individually, and this offensiveness is made worse by the fact that the acts were perpetrated literally millions of times.

242. Targeting Children More Intrusively – Defendants’ actions were highly offensive to a reasonable person because Defendants scheme to place significantly more tracking technologies on children’s websites is designed to take advantage of the plaintiffs’ vulnerability as children.

243. Violating Advertising Industry Standards – Defendants actions were highly offensive to reasonable people because they violate the online advertising industry and their own standards for respecting the personal information of children.⁶⁷

⁶⁷ These standards are found in the Self-Regulatory Principles for Online Behavioral Advertising, a standard set by the Interactive Advertising Bureau, an industry organization comprised of more than 600 leading media and technology companies, including both Defendants in this case. They are also found in the IAB’s Code of Conduct which all IAB

COUNT VIII – UNJUST ENRICHMENT

U.S. Resident Children v. All Defendants

244. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

245. Plaintiffs conferred a benefit on Defendants without Plaintiffs' consent or the consent of their parents or guardians, namely, access to wire or electronic communications and Plaintiffs' personal information over the Internet.

246. Upon information and belief, Defendants realized such benefits either through sales to third-parties or greater knowledge of its users' behavior without their consent.

247. Acceptance and retention of such benefit without Plaintiffs' consent is unjust and inequitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class Members and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class Members against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

members, including Viacom and Google, "are to required to be compliant with" to be a member of the organization. The Code of Conduct can be viewed here:
http://www.iab.net/media/file/IAB_Code_of_Conduct_10282-2.pdf (last visited July 30, 2014).

E. Permanently restrain Defendants, and their officers, agents, servants, employees, and attorneys, from tracking their users without consent or otherwise violating their policies with users;

F. Award Plaintiffs and the Class Members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

G. Order that Defendants delete the data they collected about users through the unlawful means described above; and

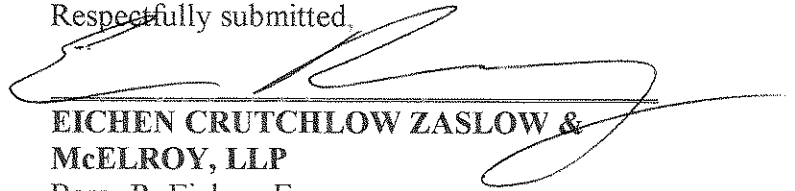
H. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: August 14, 2014

Respectfully submitted,



**EICHEN CRUTCHLOW ZASLOW &
McELROY, LLP**

Barry R. Eichen, Esq.

Evan J. Rosenberg, Esq.

40 Ethel Road

Edison, NJ 08817

Tel.: (732) 777-0100

Fax: (732) 248-8273

beichen@njadvocates.com

erosenberg@njadvocates.com

and

/s/ James P. Frickleton

**BARTIMUS, FRICKLETON,
ROBERTSON & GOZA P.C.**

James P. Frickleton, Esq.

Mary D. Winter, Esq.

Edward D. Robertson III, Esq.

11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: (913) 266 2300
Fax: (913) 266 2366
jimf@bflawfirm.com
marywinter@earthlink.net
krobertson@bflawfirm.com

Attorneys for Plaintiffs